The United States Department of the Interior Office of Inspector General Federal Information Security Management Act Fiscal Year 2011 Performance Audit



November 15, 2011





KPMG LLP 2001 M Street, NW Washington, DC 20036-3389

November 15, 2011

Mr. Eddie Saffarinia
Assistant Inspector General for Information Technology
U.S. Department of the Interior
Office of Inspector General
1849 C Street, NW MS 4428
Washington, DC 20240-0001

Dear Mr. Saffarinia:

This report presents the results of our work conducted to address the performance audit objectives relative to the Fiscal Year (FY) 2011 Federal Information Security Management Act (FISMA) Audit for Unclassified Systems. We performed our work during the period of April 24 to October 7, 2011 and our results are as of November 15, 2011.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit objective(s) of our work were to conduct an independent audit of the information security program and practices of the U.S. Department of the Interior (DOI) to determine the effectiveness of such programs and practices for the year ending September 30, 2011. Specifically, the objectives of the audit were to:

- Perform the annual independent FISMA audit of DOI's information security programs and practices related to the financial and non-financial information systems in accordance with the FISMA, Public Law 107-347.
- Assess the implementation of the security control catalog contained in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev (Rev) 3. We utilized key criteria and guidance, including Federal Information Processing Standard (FIPS) Publication (PUB) 199, FIPS PUB 200, NIST SP 800-37 Rev 1, and NIST SP 800-53 Rev 3. Key criteria and guidance were used to evaluate DOI's implementation of the risk management framework and the extent of implementation of select security controls.
- Prepare responses for each of the Department of Homeland Security (DHS) CyberScope FISMA
 Questions on behalf of the DOI Office of Inspector General (OIG) to support documented conclusions
 with appropriate rationale/justification as to the effectiveness of the information security program and
 practices of the DOI for each area evaluated and overall.



Our procedures tested security control areas identified in NIST SP 800-53 and additional security program areas identified in the 2011 CyberScope FISMA Questionnaire for the OIG. Of the 15¹ Bureaus and Offices within the scope of our 2011 FISMA procedures, we excluded the OIG systems to avoid the appearance of a conflict and selected a sample of 10% of the remaining DOI systems. Our sample resulted in a set of systems distributed over 12 Bureaus/Offices. These Bureaus/Offices are, the Bureau of Indian Affairs (BIA), the Bureau of Land Management (BLM), Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE), the Bureau of Reclamation (BOR), the U.S. Fish and Wildlife Service (FWS), the National Business Center (NBC), the National Park Service (NPS), the Office of the Hearings and Appeals (OHA), the Office of Historical Trust Accounting (OHTA), the Office of Surface Mining Reclamation and Enforcement (OSM), the Office of the Special Trustee for American Indians (OST), and the United States Geological Service (USGS). At the conclusion of our test procedures, we aggregated the individual Bureau and system results by control area to produce results at the Department level.

The DOI has established and is maintaining security programs for IT risk management, security configuration management, incident response, security training, Plans of Action and Milestones (POA&Ms), remote access, identity and access management, continuous monitoring, contingency planning, contractor systems, and security capital planning. However, while the cyber security training and security capital planning programs were consistent with applicable FISMA requirements, OMB policy, and applicable NIST guidelines, significant improvements are needed for the rest of the previously mentioned program areas.

As part of on-going efforts to improve its security program and better manage fiscal resources, the DOI launched an IT Transformation initiative in December 2010 through Secretarial Order #3309. This initiative aims to realign IT operations, minimize duplication, improve services, and reduce costs. This multi-year program is currently in the early stages of deployment. Its implementation provides the opportunity to improve IT governance, realign and update DOI IT security policies and procedures, and improve stakeholder accountability for the uniform implementation of the updated IT security policies and procedures.

We observed that most deficiencies stem from incomplete, outdated, or laxly enforced IT security policies at the Department level. Shortcomings in the use of the (b) (7)(E) application due to a lack of uniform guidance and procedures for its use and a poor understanding of security management roles and their responsibilities account for many of the problems identified. In addition, the Department has not followed up on all prior year findings identified in the OIG's report. Of the 32 findings reported in the 2010 OIG FISMA Report, 29 remain open.

The following table summarizes the control areas tested and our results at the Department level. Our results show that while the Department and its Bureaus and Offices have made improvements in their Information Technology (IT) controls environments we found deficiencies in 9 of the 11 areas in the 2011 CyberScope FISMA Questionnaire for the OIG. The RESULTS section of this report further details our findings, conclusions, and recommendations. In addition, APPENDIX III – 2011 CYBERSCOPE FISMA QUESTIONNAIRE RESPONSES provides the full text of the responses provided to the OIG for their response to the 2011 CyberScope questionnaire.

_

¹ This includes, Bureau of Indian Affairs (BIA), the Bureau of Land Management (BLM), Bureau of Ocean Energy Management, Regulation and Enforcement (BOEMRE), the Bureau of Reclamation (BOR), the U.S. Fish and Wildlife Service (FWS), the National Business Center (NBC), the National Parks Service (NPS), the Office of the Hearings and Appeals (OHA), the Office of Historical Trust Accounting (OHTA), the Office of Inspector General (OIG), the Office of the Secretary of the Interior (OS), the Office of Surface Mining Reclamation and Enforcement (OSM), the Office of the Special Trustee for American Indians (OST), the Office of the Solicitor (SOL), and the United States Geological Service (USGS).



	2011 FISMA	Findings/Results Summary			
	Control Area	Tildings/Results Stillings			
1.	Risk Management	OOI has established and is maintaining a risk management program.			
	gement	However, DOI has not:			
		developed and consistently implemented risk management procedures,			
		implemented a comprehensive IT governance structure,			
		implemented effective management and communication of mission/business risks, and			
		fully implemented the NIST Risk Management Framework.			
2.	Configuration Management	DOI has established and is maintaining a security configuration management program.			
		However, DOI has not:			
		fully developed and consistently implemented configuration management policies and procedures,			
		consistently documented, reviewed, and implemented standard baseline configurations,			
		consistently documented, approved, and reviewed baseline configuration deviations,			
		fully developed, documented, and consistently implemented a patch management process, and			
		mitigated system vulnerabilities consistently and timely.			
3.	Incident Response	DOI has established and is maintaining an incident response and reporting program.			
		However, DOI has not:			
		fully developed and consistently implemented detailed incident monitoring, response, and reporting procedures across the Department.			
4.	Cyber Security Training	The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines that includes:			
		documented policies and procedures for security awareness training,			
		documented policies and procedures for specialized training for users with significant information security responsibilities,			
		• security training content based on the organization and roles, as specified in agency policy or standards,			
		identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other agency users)			



		with access privileges that require security awareness training, and
		• identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other agency users) with significant information security responsibilities that require specialized training.
5.	POA&M	DOI has established and is maintaining a Plan of Action and Milestone (POA&M) program that tracks and remediates known information security weaknesses.
		However, DOI has not:
		fully developed and consistently implemented detailed POA&M procedures, and
		completed corrective actions in a timely fashion.
6.	Remote Access	DOI has established and is maintaining a remote access program.
		However, DOI has not:
		fully developed and consistently implemented detailed remote access procedures,
		fully developed and enforced a DOI-wide telecommuting policy and procedures,
		implemented a Department-wide program for the management and security of remote devices and users that includes the consistent implementation of multi-factor authentication, and
		adequately developed and implemented remote access Rules of Behavior in accordance with U.S. Federal government policies.
7.	Identity and Access Management	DOI has established and is maintaining an identity and access management program that identifies users and network devices.
	8	However, DOI has not:
		consistently implemented detailed account management procedures,
		• fully implemented user and non-user account tracking, account issuance, access privilege management, and account termination,
		consistently implemented multi-factor authentication / Personal Identity Verification (PIV) where required,
		consistently implemented authentication of network devices, and
		• fully employed the least privilege principle at all bureaus/offices.



	Continuous Monitoring	DOI has established an enterprise-wide continuous monitoring program that assesses the security state of information systems.
		However, DOI has not:
		fully developed and consistently implemented a continuous monitoring policy, an enterprise-wide monitoring strategy, and monitoring procedures, and
		uniformly implemented ongoing assessments of security controls and the use of network monitoring and vulnerability testing tools.
	Contingency Planning	DOI has established and is maintaining an enterprise-wide business continuity/disaster recovery program.
		However, DOI has not:
		consistently implemented its contingency planning policy,
		fully developed and consistently implemented contingency planning procedures,
		developed, fully implemented, and tested infrastructure recovery, system contingency, and business continuity/disaster recovery plans,
		established alternate processing sites for all systems,
		consistently implemented backup procedures in accordance with U.S. Federal government standards and guidelines, and
		developed and consistently implemented test, training, and exercise programs across the Department that include after-action reports.
	Contractor Systems	DOI has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including DOI systems and services residing in public cloud.
		However DOI has not:
		• fully developed and consistently enforced policies and procedures for the oversight of systems operated on DOI's behalf by contractors or other entities,
		completed and maintained an inventory of systems owned or operated by contractors or other entities, and
		• properly documented, authorized, and maintained interface agreements (e.g., Memoranda of Understanding (MOUs)).
	Security Capital	DOI has established and maintains a security architecture and capital planning investment program for information security that includes:
Planning		documented policies and procedures to address information security in the capital planning and investment control process,
		• information security requirements as part of the capital planning and investment process,



establishes a discrete line item for information security in organizational programming and documentation,
 employs a (b) (7)(E) to record the information security resources required, and
 ensures that information security resources are available for expenditure as planned.

We observed that, in general, most deficiencies stem from incomplete, outdated, or inconsistently enforced IT security policies at the Department level. Shortcomings in the (b) (7)(E) application, lack of uniform procedures for its use, and poor understanding of security management roles and responsibilities account for many problems regarding the implementation of the existing Department-wide IT security policies and procedures.

We have made 18 recommendations related to these control deficiencies intended to strengthen the respective Bureaus, Offices, and the Department's information security program. Overall, updating the existing DOI IT Security Policy Handbook, supplementing it with detailed procedures, and enforcing accountability for the security responsibilities of the various stakeholders should greatly improve the Department's security posture and compliance.

This performance audit did not constitute an audit of financial statements in accordance with *Government Auditing Standards*. KPMG was not engaged to, and did not, render an opinion on the U.S. Department of the Interior's internal controls over financial reporting or over financial management systems (for purposes of OMB's Circular No. A-127, *Financial Management Systems*, July 23, 1993, as revised). KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.

Sincerely,



The United States Department of the Interior Office of Inspector General

Federal Information Security Management Act - Fiscal Year 2011 Performance Audit

Table of Contents

BACKGROUND	9
Mission of the DOI and its Bureaus/Offices	9
Information Technology (IT) Organization	10
FISMA	
OBJECTIVES, SCOPE, AND METHODOLOGY	11
RESULTS	12
FINDINGS	12
Risk Management Program	12
Risk Management Program Recommendation	13
Configuration Management Process	14
Configuration Management Process Recommendation	15
Incident Response Program	15
Incident Response Program Recommendation	16
POA&M Tracking Process	16
POA&M Tracking Process Recommendation	17
Remote Access Program	18
Remote Access Program Recommendation	19
Identity and Access Management Program	19
Identity and Access Management Program Recommendation	20
Continuous Monitoring Program	20
Continuous Monitoring Program Recommendation	21
Contingency Planning Program	21
Contingency Planning Program Recommendation	
Contractor System Program	23
Contractor System Program Recommendation	
CONCLUSIONS	
MANAGEMENT RESPONSE TO REPORT	
APPENDIX I – LISTING OF ACRONYMS	
APPENDIX II – PRIOR YEAR FINDING STATUS	
APPENDIX III – 2011 CYBERSCOPE FISMA QUESTIONNAIRE RESPONSES	38

BACKGROUND

Mission of the DOI and its Bureaus/Offices

The U.S. Department of the Interior (DOI) protects America's natural resources and heritage, honors our cultures and tribal communities, and supplies the energy to power our future. DOI is currently composed of 8 Bureaus and a number of additional Offices that fall under the Office of the Secretary, the Assistant Secretary for Policy, Management and Budget, Solicitor's Office and Office of Inspector General. Of those, the following 12² Bureaus and Offices are included within the scope of the Office of Inspector General's (OIG) FISMA reporting for 2011:

- 1. The <u>Bureau of Indian Affairs (BIA)</u> Responsible for the administration and management of 55 million surface acres and 57 million acres of subsurface minerals estates held in trust by the United States for American Indian, Indian tribes, and Alaska Natives.
- 2. The <u>Bureau of Land Management (BLM)</u> Administers 262 million surface acres of America's public lands, located primarily in 12 Western States. The BLM sustains the health, diversity, and productivity of the public lands for the use and enjoyment of present and future generations.
- 3. The <u>Bureau of Ocean Energy Management</u>, <u>Regulation and Enforcement (BOEMRE)</u>³ Responsible for overseeing the safe and environmentally responsible development of energy and mineral resources on the Outer Continental Shelf.
- 4. The <u>Bureau of Reclamation (BOR)</u> Manages, develops, and protects water and related resources in an environmentally and economically sound manner in the interest of the American public.
- 5. The <u>U.S. Fish and Wildlife Service (FWS)</u> Created to conserve, protect, and enhance fish, wildlife, and plants and their habitats for the continuing benefit of the American people.
- 6. The <u>National Business Center (NBC)</u> Supports DOI Bureaus and Offices and over 150 government Offices and agencies as a Shared Service Center by providing a diverse, yet integrated, set of administrative solutions and is currently the only federal agency designated by both Office of Management and Budget (OMB) and Office of Personnel Management (OPM) as a Center of Excellence in the financial management and human resources lines of business.
- 7. The <u>National Park Service (NPS)</u> Responsible for preserving the natural and cultural resources and values of the national park system.
- 8. The Office of Hearings and Appeals (OHA) Responsible for handling administrative appeals from decisions of the Department's Bureaus and Offices, primarily decisions of contracting Officers throughout the Department and programmatic decisions of Bureaus such as the Bureau of Indian Affairs, Bureau of Land Management, Minerals Management Services, and Office of Surface Mining Reclamation and Enforcement.
- 9. The <u>Office of Historical Trust Accounting (OHTA)</u> Oversees the historical accounting to Individual Indian Money (IIM) beneficiaries mandated by the Court in Cobell v. Norton.

³ As of October 1, 2011, the Bureau of Ocean Energy Management (BOEM) and Bureau of Safety and Environmental Enforcement (BSEE) officially replaced BOEMRE.

² Of the 15 Bureaus and Offices within the scope of our 2011 FISMA procedures, we excluded the OIG systems to avoid the appearance of a conflict and selected a sample of 10% of the remaining DOI systems. Our sample resulted in a set of systems distributed over 12 Bureaus/Offices.

- 10. The Office of Surface Mining (OSM) Reclamation and Enforcement Carries out the requirements of the Surface Mining Control and Reclamation Act in cooperation with States and Tribes. Their primary objectives are to ensure that coal mines are operated in a manner that protects citizens and the environment during mining and assures the land is restored to beneficial use following mining, and to mitigate the effects of past mining by aggressively pursuing reclamation of abandoned coal mines.
- 11. The <u>Office of the Special Trustee for American Indians (OST)</u> Improves the accountability and management of Indian funds held in trust by the U.S. Federal government.
- 12. The <u>U.S. Geological Survey (USGS)</u> Serves the nation by providing reliable scientific information to describe and understand the earth; minimize loss of life and property from natural disasters; manage water, biological, energy, and mineral resources; and enhance and protect our quality of life.

Information Technology (IT) Organization

The Office of the Chief Information Officer (OCIO) heads the security management program for the Department. With some exceptions (e.g., Office of Hearings and Appeals), the Bureaus/Offices have an Associate Director for Information Resources (ADIR) whose role is roughly equivalent to that of a Bureau Chief Information Officer. Many Bureaus/Offices also have Bureau Chief Information Security Officers (BCISOs) that are responsible for the local implementation of the Department's information security program.

The DOI is currently in the midst of an IT Transformation: a multi-year program that will realign how information technology is designed, priced, and delivered in support of customer goals to achieve the Department's mission. DOI launched IT Transformation in December 2010 through Secretarial Order #3309 to realigning IT operations across the Department to minimize duplication, improve services, and reduce costs. The initiative would bring under the direct purview of the OCIO IT Infrastructure & Operations and Compliance Functions that were previously replicated across multiple Bureaus. The transformation initiative would leave only mission application support at the Bureau-level. An IT Transformation Strategic Plan was submitted to the Secretary in June 2011. The expected benefits of the IT Transformation include increased customer satisfaction, a modernized service delivery model for IT, consolidated infrastructure, improved compliance, and mission applications that stay close to the customers.

FISMA

Title III of the E-Government Act of 2002, commonly referred to as the Federal Information Security Management Act (FISMA), focuses on improving oversight of federal information security programs and facilitating progress in correcting agency information security weaknesses. FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that provides security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. The Act assigns specific responsibilities to agency heads and Inspector Generals (IGs) for compliance with FISMA requirements and oversight. The Act is supported by Office of Management and Budget (OMB) agency security policy and risk-based standards and guidelines published by National Institute of Standards and Technology (NIST), which are related to defining and implementing security requirements to protect agency information and information systems.

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems. Agency heads are also responsible for complying with the requirements of FISMA and related OMB policies and NIST procedures, standards, and guidelines. FISMA directs federal agencies to report annually to the OMB Director, Comptroller General, and selected congressional committees on the adequacy and effectiveness of agency information security policies, procedures, and practices and compliance with FISMA. In addition, FISMA requires agencies to have an annual independent evaluation performed of their information security programs and practices and to report the evaluation results to OMB. FISMA states that the independent evaluation is to be performed by the agency IG or an independent external auditor as determined by the IG.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives for this performance audit were to conduct an independent audit of the information security program and practices of the DOI to determine the effectiveness of such programs and practice for the year ending September 30, 2011. Specifically, the objectives of this audit were to:

- Perform the annual independent Federal Information Systems Security Management (FISMA) audit of DOI's information security programs and practices related to the financial and non-financial information systems in accordance with the FISMA, Public Law 107-347.
- Assess the implementation of the security control catalog contained in the NIST SP 800-53 Rev 3. We
 utilized key criteria and guidance, including FIPS 199, FIPS 200, and NIST SP 800-53 Rev 3, to evaluate
 the implementation of the risk management framework and the extent of implementation of security
 controls selected from the security control catalog.
- Prepare responses for each of the OMB/Department of Homeland Security (DHS) CyberScope FISMA
 Questions on behalf of the DOI OIG to support documented conclusions on the effectiveness of the
 information security program and practices of the DOI for each area evaluated.

The scope of our audit included the following:

- 1. An inspection of the information security practices and policies established by the DOI Office of the Chief Information Officer (OCIO)
- 2. An inspection of the information security practices, policies, and procedures in use across 12 Bureaus of the DOI, specifically, BIA, BLM, BOEMRE, BOR, FWS, NBC, NPS, OHA, OHTA, OSM, OST, and USGS

Specifically, our approach followed these three steps:

- **Step A:** Department-Level Compliance During this step we gained Department-wide understanding of the FISMA-related policies and guidance established by the DOI OCIO. We compared the policies, procedures, and practices established to the applicable Federal laws and criteria to determine the overall compliance with FISMA at the Department-level.
- **Step B:** Bureau-Level Compliance During this step we gained an understanding of the extent of the implementation of Departmental FISMA policies and procedures across the DOI's Bureaus.
- **Step C:** Assessment of the Implementation of Select Security Controls from the NIST SP 800-53 Rev 3 During this process we assessed the implementation of a selection of security controls from the NIST SP 800-53 Rev 3, for our representative subset (10 %) of DOI's information systems. The controls selected were chosen to address all the areas covered by the DHS FY2011 Inspector

General Federal Information Security Act Reporting (CyberScope Questions) and additional controls selected to follow up on deficiencies identified in the prior year OIG FISMA assessment.

The DOI Statement of Work (SOW) for the FISMA audit required us to perform our procedures on a representative subset of systems defined as at least 10% of the information systems in the DOI's authoritative system inventory on the (b) (7)(E)

RESULTS

We observed that DOI is undertaking actions to improve its overall IT Governance and security posture. These activities are anchored in the Department's IT Transformation initiatives as outlined in the IT Transformation Strategic Plan. The DOI IT Transformation was launched in December 2010 through Secretarial Order #3309 with the main goals of realigning IT operations across the Department to minimize duplication, improve services, and reduce costs. Management's expected benefits of the IT Transformation include increased customer satisfaction, a modernized service delivery model for IT, consolidated infrastructure, improved compliance, and mission applications that stay close to the customers.

We observed that DOI has established and is maintaining programs for IT risk management, security configuration management, incident response, security training, Plans of Action and Milestones (POA&Ms), remote access, identity and access management, continuous monitoring, contingency planning, oversight of systems operated on its behalf by contractors or other entities, and security capital planning. As noted in our follow-up of prior-year issues, we noted improvements in DOI's security program that include:

- 1. The Department issued a Memorandum to affirm that (b) (7)(E)
- 2. The Department issued guidance for the 2011 Internal Control Reviews (ICR) process that incorporates NIST 800-53 Rev 3 controls. (b) (7)(E) with 800-53 Rev 3 controls and this permitted the results of ICR testing of Rev 3 controls to be recorded in (b) (7)(E).
- 3. All POAM's are required to be entered and maintained in (b) (7)(E) and reported to OCIO on a (b) (7)(E) and bureaus/offices generally comply with this requirement.
- 4. OS/ISD now monitors all changes to the DOI network on a daily basis using (b) (7)(E)

Our audit also identified areas where the Department needs to make improvements in their overall security program. Security program areas were improvements are needed are IT risk management, security configuration management, incident response, Plans of Action and Milestones (POA&Ms), remote access, identity and access management, continuous monitoring, contingency planning, and oversight of systems operated on its behalf by contractors or other entities.

FINDINGS

Risk Management Program

The NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems established guidance for the development of a risk management framework. The NIST framework provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Ongoing monitoring is a critical part of that risk management process. Further, the DOI (b) (7)(E) developed by the OCIO and provided to the Bureaus states:

Bureaus and Offices shall conduct assessments of the risk and magnitude of harm that could result from the unintentional and/or unauthorized access, use, disclosure, disruption, modification, or

destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).

We observed the following weaknesses in DOI's Risk Management program:

- DOI policies include elements to support a risk management approach; however, they have not been integrated into a comprehensive risk management framework for DOI that is fully consistent with NIST SP 800-37 Rev 1.
- 2. The DOI (b) (7)(E) has not been updated to incorporate NIST SP 800-53 Rev 3 guidance, which should provide the basis for all security assessments.
- 3. Security documentation, including risk assessment documentation for systems, is recorded inconsistently on and therefore management cannot readily assess the completion status of security management activities and assess the quality of the information recorded.
- 4. Security control baselines are not tailored to individual systems. The controls documented in the generated System Security Plans (SSPs) are exact copies of NIST 800-53 control baselines.

While the ITSPH identifies a hierarchy of roles and responsibilities that are involved with the assessment of system, mission, and organizational risks, it does not provide an overall strategy, plan, and process for IT governance and risk management. Further, DOI policies and procedures do not provide sufficiently detailed guidance for the uniform use of the (b) (7)(E) tool. Security documentation is still recorded inconsistently on and this makes it harder to track the completion of security management activities and assess the quality of the information available. At present, (b) (7)(E) does not permit direct entry of information on the implementation of security controls, but instead uses the results of Internal Control Review (ICR) assessments to populate the System Security Plan (SSP) controls fields.

As a result, the lack of properly documented policies and procedures could cause critical controls to not be implemented or evaluated, systems security plans not addressing current risks and issues and non-compliance with NIST guidance. Further, missed or improperly implemented controls may result in unknown or unmanaged increase in overall risk to DOI systems.

Risk Management Program Recommendation DOI should:

- a. Update the DOI (b) (7)(c) to meet NIST SP 800-37 Rev 1, NIST SP 800-53 Rev 3, and other current U.S. Government policies and guidance for IT Governance and Risk Management.
- b. Update DOI procedures to consolidate risk management framework implementation guidance and foster the uniform implementation of risk management activities across the Department. This should include providing clear usage guidelines for the identification of systems and authorization boundaries, use of a consistent documentation recording structure to help make system documentation easier to find, and labeling system operational status consistently.
- c. Require Bureaus to update documentation to include accurate system boundary information (i.e., FISMA Children), risk assessments and security assessment reports, and POA&Ms.

d. Implement procedures to help ensure that the controls documented in the Security Plans (SSPs) accurately represent the control baseline tailored for each system and the actual implementation of those controls.

Configuration Management Process

Consistent with NIST guidance, the (b) (7)(E), Section CM-1 Configuration Management Policy and Procedures and CM-6, Configuration Settings state that the organization should:

- Establish and documents mandatory configuration settings for information technology products employed within the information system using [Assignment: organization-defined
- security configuration checklists] that reflect the most restrictive mode consistent with operational requirements;
- Implements the configuration settings;
- Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational
- · requirements; and
- Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Further, the (b) (7)(E) goes on to indicate in Section SI-2, Flaw Remediation that Bureaus and Offices shall identify, report, and correct all information system flaws.

We observed the following weaknesses in DOI's Configuration Management program:

- 1. Configuration management procedures are not fully developed and consistently implemented throughout the Department. Some Bureaus have been proactive in acquiring automated configuration management tools, in upgrading legacy systems to enable centralized management, and in having procedures that enforce a limited number of standard configurations. Others have extensive variations in security configurations on (b) (7)(E) and on (b) (7)(E). Many of the security configuration deviations are approved by local system owners, or field Offices, with limited challenge to the deviation. Leaving the approval of the deviations to the local level has prevented the use of centralized configuration management tools for standardization, verifying compliance and patching across the Department.
- 3. The Department has not fully developed its hardware inventory and has not standardized on an hardware detection and inventory tool.
- 4. The Department conducts vulnerability scans monthly and provides the results to the Bureaus/Offices that have chosen to participate in the program. However, the Department does not scan the entire infrastructure. It is usually up to the Bureau/Office to analyze the output of the scans, and determine appropriate action, but we noted these reviews are sometines conducted after the scan results have gone

stale. Further, Bureaus/Offices have implemented scanning capabilities using a variety of products, which produce different kinds of output, and can be difficult to correlate. Some Bureaus/Offices monitor the output of their automated systems very closely, but others have a more ad hoc approach. In addition, scanning is not performed with authenticated credentials, which will provide more accurate and detailed results.

- 5. Bureaus/Offices have deployed Federal Desktop Core Configuration (FDCC)/United States Government Configuration Baseline (USGCB) security configurations with Bureau/Office determined deviations to their workstations. Each Bureau/Office has processes for approving deviations; however, those processes vary widely, from permitting only deviations that are standard for the entire Bureau to permitting workstation-by-workstation deviations. Many Bureaus lacked a frequently updated baseline security configuration that specifies all approved deviations for all systems and could be used to scan for compliance. DOI lacks specific guidance and criteria for what constitutes compliance, how to scan consistently for it, and how to report.
- 6. Bureaus/Offices had vulnerability management processes ranging from organized, mature to ad-hoc. Bureaus/Offices had no consistent guidance on the use of vulnerability scanning tools. Almost all tools were able to report issues relating to software patches, but some were not configuring their tools with proper permissions for the scans. Vulnerability remediation has not kept up with vulnerability scanning.
- 7. Operating system patches were not timely installed at some DOI Bureaus and Offices that remediate operating system vulnerabilities and third-party applications. Most of the Bureaus/Offices were not applying third-party application patches in a timely manner. Bureaus also prioritized operating system patches over third-party application patches, even when they have the same risk rating. Tools to handle the third-party patches were often in place but used inconsistently.

A standardized configuration management policy and procedures, that include a standard configuration management deviation process, tools to be used, guidance on tool configuration, and guidance on implementation of standard configurations by operating system and application has not been implemented at each Bureau or Office. This has resulted in inconsistent implementation of operating system and third party application configurations that could expose operating systems and applications to attacks, unauthorized modification, virus infection, or data compromise. Further, the lack of consistent baseline configurations across the Department could result in systems operating with unknown or improperly configured settings.

Configuration Management Process Recommendation

DOI OCIO should update and issue policies and procedures to each Bureau/Office to standardize the configuration management process across all Bureaus/Offices. These policies and procedures should include security technical implementation guidance (STIG) for the operating systems and applications within the Department and those managed by external entities. Further, the configuration management policy and procedures should provide a standard DOI-approved scanning tool kit, to include report templates and general configuration information that provides approved automated tools needed to scan operating systems and applications periodically for appropriate configurations. DOI should also deploy (b) (7)(E) Department-wide to automate the collection and reporting of inventory and other security information.

Incident Response Program

The DOI *Information Technology Security Policy Handbook*, Section IR-1, Incident Response Policy and Procedures that are consistent with NIST guidance states that Bureaus and Offices shall develop, disseminate, and periodically review and update:

- Formal, documented, incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

The following weakness was noted in the Department's Incident Response policies and procedures:

1. The DOI Computer Security Incident Response Handbook provides response and reporting procedures for the Department, but some Bureaus have implemented these procedures inconsistently.

The cause of the weakness relates to individual employees interpreting the DOI Incident Response procedures differently depending on the circumstances or following other procedures altogether. We noted that the level of detail in reports to Computer Incident Response Center (CIRC) varies significantly.

The lack of consistent implementation of documented policies may result in an incident going undetected, not properly reported to management, or ineffective handling of incidents. At any time, Bureau personnel might be following Bureau reporting guidelines, the DOI (b) (7)(E) and/or the Computer Incident Response Handbook, or none of the above.

Incident Response Program Recommendation

DOI OCIO should:

- 1. Review Incident Response Policies to help ensure that all Bureaus are identifying, analyzing, and reporting incidents consistently so that they may be properly addressed, shared, and communicated Department wide.
- 2. Require Bureaus to follow a common set of procedures that are consistent with the Departmental policies and procedures. Bureaus that need to deviate from the DOI-wide incident handling procedures should document the needed deviation and obtain a waiver. Any deviations should be minimal and rely on common monitoring and reporting tools with only a very small set of implementation-specific procedures to account for program and infrastructure differences.

POA&M Tracking Process

The DOI *Information Technology Security Policy Handbook*, Section CA-5 Plan of Action and Milestones, The DOI POA&M Process Standard, states:

The standard details the process and minimum mandatory implementation requirements for completion of POA&Ms by all DOI Bureaus and Offices in accordance with guidance issued by the OMB. In addition, the DOI POA&M Process Standard describes DOI-specific requirements that are necessary for the consistent and comprehensive completion of required updates to all IT security POA&Ms and establishes reporting formats for POA&Ms. Updates to POA&M status should be reported and reconciled monthly as outlined in Bureau or Office internal policy. Updates to POA&M status and metrics are required to be sent to OMB on a (b) (7)(E). As the schedule for required reporting of POA&M updates and metrics status to OMB changes frequently, updates to DOI required reporting dates shall be promulgated annually by the CSD.

The following weaknesses were noted in reviewing the Department's (POA&M) policies and procedures:

1. The U.S. Department of the Interior Plan of Action and Milestones (POA&M) Process Standard, version (b) (7)(E), incorporates procedures for the use of (b) (7)(E)

(b) (7)(E) tool for automating the process. While the procedures outline considerations regarding the prioritization of corrective actions, they lack specificity regarding the process for managing the assignment of resources based on risk related priorities and resource constraints.

- Although the procedures in the POA&M Process Standard require the tracking of the source of all POA&Ms, we found POA&Ms had not consistently identified the source of the control weakness they address.
- 3. The estimated remediation costs were not always associated with POA&M weaknesses.
- 4. Milestone and remediation dates are commonly not met.
- 5. Some entries were listed with a planned completion date well past the due date.
- 6. The DOI POA&M Process Standard requires that POA&Ms be reviewed and updated at least quarterly. However, some Bureaus have not implemented consistent management reviews to track POA&M progress and POA&Ms remain open without apparent progress.

It appears the POA&M process is not fully understood at all Bureaus, and that DOI guidance does not foster clear delineation of accountability for the tracking and completion of corrective actions. DOI guidance does not provide uniform procedures and tools for prioritizing corrective action in a way that takes in consideration both the criticality of the issues, return on investment, and resource availability. POA&M items are not properly documented or periodically reviewed to make sure information is accurate, costs are tracked, and milestones are met.

Failure to properly recognize the need for evaluating criticality, Return on Investment (ROI), and costs when prioritizing corrective action, could lead to setting unrealistic deadlines, which might explain the missed deadlines and the lack of follow-up. Further, if management's decisions on corrective action are based on inaccurate information the result could be budget overruns, inaccurate completion estimates, and security issues that remain unresolved.

POA&M Tracking Process Recommendation

DOI should improve its POA&M procedures and guidance to help ensure that:

- They provide sufficient detail regarding the prioritization of corrective actions based on risk related priorities and resource constraints and cost-effectiveness;
- The information entered when developing and updating POA&Ms is correct, complete, and includes traking the source of all POA&Ms;
- 3. Senior management is regularly provided accurate POA&M information and updates;
- 4. Senior management reviews and signs off on all POA&M entries; and
- Managers consider return on investment and costs, as well as criticality, when ranking of corrective action priorities at the system and the Bureau level to help reduce missed completion deadlines.

Remote Access Program

NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations, AC-17: Remote Access states that

The organization: a.) Documents allowed methods of remote access to the information system; b.) Establishes usage restrictions and implementation guidance for each allowed remote access method; c.) Monitors for unauthorized remote access to the information system; d.) Authorizes remote access to the information system prior to connection; and e.) Enforces requirements for remote connections to the information system.

Further, NIST 800-46, Guide to Telework and Remote Access Security states the below:

- **Section 5.1:** "...A telework security policy should define which forms of remote access the organization permits, which types of telework devices are permitted to use each form of remote access, the type of access each type of teleworker is granted, and how user account provisioning should be handled. It should also cover how the organization's remote access servers are administered and how policies in those servers are updated. The telework security policy should be documented in the system security plan."
- **Section 4.2**: "Many organization-controlled telework consumer devices can have their security managed centrally, at least to some degree...Security capabilities and appropriate actions vary widely by device type and specific products, so organizations should provide guidance to device administrators and users who are responsible for securing telework consumer devices on how they should secure them."
- **Section 3.3:** "To ensure that access is restricted properly, remote access servers should authenticate each teleworker before granting any access to the organization's resources, and then use authorization technologies to ensure that only the necessary resources can be used. Authentication can also be used to confirm the legitimacy of telework client devices and remote access servers. Access control technologies are also needed to restrict access to network communications and applications."
- Section 2.2: "Organizations have many options for providing remote access to their computing resources. For the purposes of this publication, the remote access methods most commonly used for teleworkers have been divided into four categories based on their high-level architectures: tunneling, portals, remote desktop access, and direct application access... When planning a remote access solution, organizations should carefully consider the security implications of the remote access methods in each category, in addition to how well each method may meet operational requirements."

The following weaknesses were noted in DOI's remote access program:

- 1. Remote access procedures were not fully developed and sufficiently detailed. Most DOI Bureaus and Offices are using the Department's remote access service to establish virtual private network (VPN) connections (b) (7)(E)

 Because the Bureaus have cited interoperability problems with the PIV cards already issued and significant numbers of remote access users do not yet hold PIV cards, the Department has left the decision up to the individual Bureaus and Offices as to whether use of the PIV card for 2-factor authentication for remote access is mandatory.

 (b) (7)(E)

 does not adequately meet U.S. Federal government requirements for two-factor identification and authentication.
- Telecommuting policy and procedures are not fully developed or implemented in accordance with U.S.
 Federal government policies. Some DOI components have made the implementation and use of a PIV
 card mandatory within a limited timeframe while other components have not. In addition, although DOI
 policies permit only U.S. Federal government furnished equipment (GFE) to be used for remote access,

in practice this policy is not enforced and both personal equipment and the equipment of non-federal users is permitted.

- 3. The Agency does not adequately monitor remote devices when connected to the agency's networks remotely in accordance with U.S. Federal government policies. The Department has implemented several types of intrusion detection and intrusion prevention capabilities. However, it does not have the capability to verify that the remote devices and software have a compliant security configuration.
- 4. Remote access rules of behavior were not adequate in accordance with U.S. Federal government policies. The DOI IT Security Policy Handbook requires rules of behavior (ROB) to cover remote access. We found DOI does not have consistent Remote Access Rules of Behavior throughout the Department.

DOI management has not fully developed and uniformly implemented remote access policies, procedures, and rules of behavior that meet U.S. Federal government standards and guidelines.

A lack of fully developed and uniformly implemented remote access policies, procedures, and rules of behavior expose DOI networks and information resources to multiple threats that include unauthorized access, denial of service, and exposure of personal and otherwise sensitive information.

Remote Access Program Recommendation

DOI management should strengthen the implementation, control and security of its remote access program in compliance with NIST 800-53 Rev 3, NIST 800-46 requirements, HSPD 12, and other relevant U.S. Federal government requirements thereby mitigating risks to DOI and Bureau information systems and data.

Identity and Access Management Program

NIST SP 800-53: *Recommended Security Controls for Federal Information Systems and Organizations*, AC-2: Account Management states that the organization manages information system accounts, including:

- 1. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
- 2. Establishing conditions for group membership;
- 3. Identifying authorized users of the information system and specifying access privileges;
- 4. Requiring appropriate approvals for requests to establish accounts;
- 5. Establishing, activating, modifying, disabling, and removing accounts;
- 6. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- 7. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;
- 8. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
- 9. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and
- 10. Reviewing accounts [Assignment: organization-defined frequency].

Further, Homeland Presidential Security Initiative (HSPD) -12 - *Policy for a Common Identification Standard for Federal Employees and Contractors*; requires a mandatory, government-wide standard for secure and reliable forms of identification issued by the federal government to its employees and to the

employees of federal contractors. The implementation of this Standard will ensure the identification for government employees and contractors is reliable and secure. Agencies must ensure consistency with existing privacy and security law and policies to ensure employee and contractor information is protected and appropriately used.

We noted the following in performing a review of the DOI's identity and access program:

- 1. Account Management policy is not consistently implemented. Even though (b) (7)(E) is implemented at the Department level and the Department's DOI (b) (7)(E) provided a standardized account management process, neither nor the DOI (b) (7)(E) is adopted and used to provide a consistent process for the identification and management of non-federal users (contractors and non-federal employees) and the management of (b) (7)(E) (e.g. (b) (7)(E)).
- Account management procedures are not consistently implemented in accordance with U.S. Federal government policies.
- 3. Accounts were not properly terminated when users no longer required access. In 3 of the 12 Bureaus and Offices reviewed, we identified users whose accounts had not been appropriately terminated when users no longer required access.
- 4. DOI has not adequately planned for the implementation of PIV for logical access in accordance with U.S. Federal government policies. Legacy systems remain in some Bureaus that are not capable of using the PIV card in situations where two-factor authentication is required (e.g. for privileged access).
- 5. The principle of least privilege is not being fully employed at all bureaus/offices.
- Network devices are not properly authenticated. Automated techniques and tools, such as Network
 access control (NAC) and media access code (MAC) controls that can be used to identify devices that
 connect to a network, have not been consistently implemented.

DOI management has not fully developed and uniformly implemented identity and access management policies, procedures, and rules of behavior that meet U.S. Federal government standards and guidelines, and ensured sufficient protection against unauthorized access to DOI information systems, adequate segregation of duties in job functions, and controlled access to devices on the DOI network.

The lack of a fully developed, uniformly implemented, and continuously monitored identity and access management program exposes DOI networks and information resources to the risk of unauthorized access and the security, reputational, and operational consequences that may result.

Identity and Access Management Program Recommendation

DOI management should strengthen the implementation of its identity and access management program to comply with NIST 800-53 Rev 3, HSPD 12, and other relevant U.S. Federal government requirements. Improvements should address Departmental policies and procedures, user rules of behavior, access reviews for segregation of duties, Department-wide PIV implementation and use for user 2-factor authentication, and proper device identification and authentication.

Continuous Monitoring Program

NIST SP 800-53: Recommended Security Controls for Federal Information Systems and Organizations, CA-7: Continuous Monitoring states that organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:

- 1. A configuration management process for the information system and its constituent components;
- 2. A determination of the security impact of changes to the information system and environment of operation;
- 3. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and
- 4. Reporting the security state of the information system to appropriate organizational officials.

The following was noted in DOI's continuous monitoring program:

- A continuous monitoring policy is not fully developed or consistently implemented. A comprehensive
 continuous monitoring policy or strategy does not exist, although the Department has implemented an
 Internal Controls Review (ICR) process that requires an annual review of one third of NIST 800-53 Rev
 3 controls. In addition, continuous monitoring procedures are not consistently implemented and no
 specific procedures or guidance exists at the Department level for the consistent performance of network
 monitoring or vulnerability assessments.
- 2. The ICR process has been in place for several years, but it is not uniformly implemented and stable. Network monitoring and automated vulnerability testing tools are not used consistently across all bureaus/offices.

DOI management has not developed and implemented a comprehensive continuous information system monitoring process to ensure ongoing and consistent updates to component information security plans, security assessment reports and associated management reporting.

Without a well-defined and well-implemented continuous monitoring policy and strategic plan, the risk is increased that DOI information systems will be subject to uncontrolled or unapproved configuration system changes and management reporting will be incomplete and/or inaccurate regarding the security state of DOI systems.

Continuous Monitoring Program Recommendation

DOI management should:

- 1. Implement a complete and consistent continuous monitoring process throughout all DOI Bureaus and Offices.
- 2. Update the existing continuous monitoring strategy to address an on-going testing of security controls and the use of automated vulnerability scanning and network monitoring.

Contingency Planning Program

The DOI *Information Technology Security Policy Handbook*, Section CP-1, Contingency Planning Policy and Procedures that is consistent with NIST guidance states that Bureaus and Offices shall develop, disseminate, and periodically review and update:

- 1. Formal, documented, contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- 2. Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

Further, the DOI *Information Technology Security Policy Handbook*, Section CP-2, Contingency Plan states that:

Bureaus and Offices shall develop and implement contingency plans for all information systems that address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organization [System Owners and Designated Approving/Accrediting Authorities] shall review and approve contingency plans and distribute copies of the plan to key contingency personnel.

We observed the following weaknesses in DOI's Contingency Planning program:

- Contingency planning activities did not take place during the transition of IT operations for the Office of Historical Trust Accounting (OHTA) to the Office of the Special Trustee for American Indians (OST).
- 2. While the systems in our sample had contingency plans consistent with NIST 800-34 Rev 1, OHTA and OS-ISD have not identified alternate processing sites and therefore their contingency plans could not be considered fully developed. Both Bureaus have open POA&Ms for the lack of alternate processing sites.
- 3. Bureau recovery strategies and plans have not been documented. System IT Contingency Plans have been completed as part of the system authorization process; however, those plans do not incorporate enterprise-wide plans. The system contingency plans reviewed do not establish a coordinated recovery strategy for Bureau information systems and operations.
- 4. Contingency Plans for Bureaus NBC / OS, OHTA and BLM (b) (7)(E)
- 5. A set of backups at FWS (b) (7)(E) and the backup process was (b) (7)(E) (b) (7)(E) . We noted that FWS (b) (7)(E) that would have flagged this problem for remediation.
- 6. None of the DOI contingency planning guidance reviewed addressed supply chain threats.
- Contingency or business continuity training, testing, and exercises have not been fully developed and thus not implemented. Business continuity testing was not documented and therefore not conducted at NBC.
- 8. NBC did not test their business continuity/disaster recovery plans this year and therefore no after-action report was produced.

DOI Contingency Plan guidance to the Bureaus is incomplete and therefore some Bureaus do not have reliable contingency and continuity processes in place. For example, DOI guidance does not require Bureaus to test backups regularly, establish a connection between system level and Bureau-wide business continuity and contingency planning, or require Bureaus to identify alternate processing sites that do have the same environmental risks as the main processing sites. Further, procedures have not been established that require management to request an approved deviation from the OCIO policy if the continuity testing is not planned and performed annually.

A lack of uniform and complete contingency planning and continuity guidance exposes DOI and its Bureaus to potential loss of data, extended down-time, and budget overruns making up for lost data.

Contingency Planning Program Recommendation

DOI management should strengthen the implementation, control and security of its policies surrounding contingency planning. Specifically, DOI should address the testing of contingency plans including the periodic testing of system backups. Alternate sites should be selected for systems with a High rating and the

systems contingency plan updated and tested to determine if the alternate site procedures will timely restore system operations.

Contractor System Program

The NIST SP 800-53 Rev 3, Section PM-5, Information System Inventory states that the organization develops and maintains an inventory of its information systems.

The following was noted in performing a review of the Department's continuous monitoring program:

- 1. The DOI Information Technology Security Policy Handbook V3.1 does not adequately define contractor oversight responsibilities and provides limited details regarding requirements for performing contractor oversight. Six of the twelve Bureaus and Offices have contractor systems in the oversight of a combined eighteen contractor systems. Of the six Bureaus that have contractor systems, only OHTA has augmented the DOI policies with their own policies.
- 2. The inventory of contractor systems is not complete at six Bureaus that have identified contractor systems.
- 3. No interfaces were shown in (b)(7)(E) interface inventory for any of the contractor systems operated for Departmental headquarters elements. We found that contractor interfaces were usually described in presystem security plans, but the Department's shift to using to create System Security Plans means those are being phased out.

DOI management has not ensured that contractor operated systems are adequately inventoried, controlled and follow the NIST requirements. A lack of well-defined and documented system inventory including a listing of interfacing systems could lead to systems being overlooked during routine audits.

Contractor System Program Recommendation

DOI management should strengthen policies and procedures for contractor managed systems to include monitoring system security, compliance with NIST requirements, and obtaining evidence that contractor-managed systems have tested security requirements.

CONCLUSIONS

DOI has established and is maintaining security programs for IT risk management, security configuration management, incident response, security training, Plans of Action and Milestones (POA&Ms), remote access, identity and access management, continuous monitoring, contingency planning, oversight of systems operated on its behalf by contractors or other entities, and security capital planning. The Department has a robust training program and an established program for security capital planning. However, DOI needs to make significant improvements to 9 of these 11 security program areas as identified above. The 9 areas that require improvement are Risk Management, Configuration Management, Incident Response, POA&Ms, Remote Access, Identity and Access Management, Continuous Monitoring, Contingency Planning, and Contractor Systems.

We observed that most deficiencies stem from incomplete, outdated, or inconsistently enforced IT security policies at the Department level. Shortcomings in the use application due to lack of uniform guidance and procedures for its use and poor understanding of security management roles and their responsibilities account for many of the problems identified regarding the implementation of the existing DOI IT security policies. Officials at several Bureaus complained that while the Department discourages the development of local security policies and procedures to foster uniformity in security practices, they are not filling existing

gaps in the guidance on activities such as system decommission and uniform procedures for documenting security management activities in (b) (7)(E).

While realignment and consolidation efforts under the DOI IT Transformation initiative should result in improvements to the Department's IT Governance, more cost-effective IT operations, and potentially better security controls, implementation of the IT Transformation is still in the early stages.

The Department has not followed up on all prior year findings identified in the OIG's report. Of the 32 findings reported in the 2010 OIG FISMA Report, 28 remain open. Please see APPENDIX II – PRIOR YEAR FINDING STATUS for a complete list.

MANAGEMENT RESPONSE TO REPORT

The DOI Office of the Chief Information Officer agreed verbally to the report and approved its issuance to meet the OIG's November 15, 2011 reporting deadline.

APPENDIX I – LISTING OF ACRONYMS

Acronym	Definition
AC	Access Control
AD	Active Directory
ADIR	Associate Director for Information Resources
AT	Awareness and Training
ATO	Authority to Operate
BCISO	Bureau Chief Information Security Officer
BIA	Bureau of Indian Affairs
BIA	Business Impact Assessment or Business Impact Analysis
BLM	Bureau of Land Management
BOEMRE	Bureau of Ocean Energy Management Regulation and Enforcement
BOR	Bureau of Reclamation
BY	Budget Year
C&A	Certification and Accreditation
CA	Security Assessment and Authorization
CIO	Chief Information Officer
CIRC	Computer Incident Response Center
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
СР	Contingency Planning
(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)

Acronym	Definition	
CSD	Cyber Security Division	
CSIRC	Computer Security Incident Response Capability	
(b) (7)(E)	(b) (7)(E)	
DHS	Department of Homeland Security	
DOI	U.S. Department of the Interior	
EID	Enterprise Infrastructure Division	
(b) (7)(E)	(b) (7)(E)	
(b) (7)(E)	(b) (7)(E)	
FCD	Federal Continuity Directive	
FDCC	Federal Desktop Core Configuration	
FIPS	Federal Information Processing Standards	
FISMA	Federal Information Security Management Act	
FWS	US Fish and Wildlife Service	
FY	Fiscal Year	
GAO	Government Accountability Office	
GAS	Government Auditing Standards	
GFE	Government Furnished Equipment	
(b) (7)(E)	(b) (7)(E)	
HSPD	Homeland Security Presidential Directive	
IA	Identification and Authentication	
ICR	Internal Controls Review	
IG	Inspector General	
IIM	Individual Indian Money	
IR	Incident Response	

Acronym	Definition
ISD	Infrastructure Services Delivery
ISSO	Information System Security Officer
IT	Information Technology
(b) (7)(E)	DOI(b) (7)(E)
KPMG	KPMG LLP
LAN	Local Area Network
MA	Maintenance
MAC	Media Access Code
MOU	Memorandum of Understanding
MP	Media Protection
NAC	Network Access Code
NBC	National Business Center
NFR	Notice of Finding and Recommendations
NIST	National Institute of Standards and Technology
NPS	National Park Service
OCIO	Office of the Chief Information Officer
ОНА	Office of Hearings and Appeals
ОНТА	Office of Historical Trust Accounting
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
OS	Office of the Secretary
OS	Operating System
OS-ISD	Office of the Secretary – Infrastructure Services Delivery

Acronym	Definition	
OSM	Office of Surface Mining Reclamation and Enforcement	
OST	Office of the Special Trustee for American Indians	
P2P	Peer-to-Peer	
PE	Physical and Environmental Protection	
PII	Personally Identifiable Information	
PIV	Personal Identity Verification	
PL	Planning	
PM	Program Management	
POA&M	Plan of Action and Milestones	
PS	Personnel Security	
PUB	Publication	
PY	Prior Year	
RA	Risk Assessment	
Rev	Rev	
RMF	Risk Management Framework	
ROB	Rules of Behavior	
ROI	Return on Investment	
SA	System and Services Acquisition	
SC	System and Communication Protection	
(b) (7)(E)	(b) (7)(E)	
SI	System and Information Integrity	
(b) (7)(E)	(b) (7)(E)	
SOL	Office of the Solicitor	
SOW	Statement of Work	

Acronym	Definition
SP	Special Publication
SSP	System Security Plan
STIG	Security Technical Implementation Guide
(b) (7)(E)	(b) (7)(E)
US	United States
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
USGS	US Geological Survey
VPN	Virtual Private Network

APPENDIX II – PRIOR YEAR FINDING STATUS

No.	IT Security Program Areas	Deficiencies	Recommendations	Disposition
1.	IT Inventory	Confusion among Bureaus to which system, (b) (7)(E) to manage IT inventory	Standardize the use of terms within (b) (7)(E)	CLOSED District is no longer in use. The Department issued a memorandu (b) (7)(E)
2.	IT Inventory	Inventory of systems are inaccurate, incomplete, and unreliable for identifying accreditation boundaries	Establish clear guidance for managing IT assets system inventory, including: the identification and documentation of minor applications, the identification (description, hosted, or operated) and documentation of contractor components, a process for adding systems in development to inventory, a process for adding test systems into inventory, and a process for mapping all components to authorization boundaries.	OPEN We noted instances, such as (b) (7)(E) at FWS and (5)(7)(E) at BOR, where the documentation found in (6)(7)(E) of the subordinate systems within the subordinate systems within the accreditation boundary was incomplete or did not exist. Additionally, some entries in the (b) (7)(E) inventory did not represent actual systems. Instead, they were just used to collect controls documentation that applies to several systems and applications joined within one accreditation boundary out of convenience and not necessarily because they share common controls.
3.	IT Inventory	Bureaus do not consistently identify IT systems or subsystems as a contractor system in inventory	Develop guidance to determine criteria for identifying contractor systems in IT inventory, separate from agency- owned systems	Although there is a field in (b) (f)(5) to indicate whether a system is a contractor system or not, there are no criteria for identifying contractor systems and security controls in the IT inventory separate from agency-owned systems and security controls.
4.	IT Inventory	Bureaus do not use consistent methods to identify their hardware and software asset inventories	Establish clear guidance for managing hardware and software asset inventory	OPEN Although some Bureaus/Offices have an automated capability to identify their hardware/software inventories, local, manual procedures are still in widespread use. There has been no Department-wide asset inventory capability put in place, and no Departmental guidance issued for the acquisition and use of automated tools with [5].(7)(E) output capability to be used to

No.	IT Security Program Areas	Deficiencies	Recommendations	Disposition
				identify hardware/software asset inventories.
5.	Certification and Accreditation	Bureaus do not have clear guidance to follow the updated NIST 800-53 Rev 3 guidance	Update DOI's security authorization policy and guidance to incorporate the latest NIST guidance (NIST 800-37, Rev 1, and NIST 800-53, Rev 3)	CLOSED The Department issued guidance for the 2011 Internal Control Reviews (ICR) process to incorporate NIST 800-53 Rev 3 controls. (b) (7)(E) with 800-53 Rev 3 controls, which permitted the results of ICR testing of Rev 3 controls to be recorded in (b) (7)(E)
6.	Certification and Accreditation	Not all systems are accredited; accreditation process for systems in development is unclear; component parts are not fully identified within a larger accreditation boundary; and not all accreditations are completed on time	Merge the multiple DOI security authorization procedural documents into a single document. The guidance should clarify when the authorization process begins in the life cycle, the role of the senior risk executive, and clarify how information system boundaries are to be documented	OPEN Although DOI has elements of a continuous monitoring strategy in place that replace the 3-year C&A re-accreditation cycle, such as the requirement for annual Internal Control Reviews (ICR), it has not established and overall Risk Management Framework that identifies the roles, responsibilities and procedures at all levels of the DOI hierarchy for continuous monitoring, risk assessment, reporting to management and re-authorization of systems.
7.	Security Configuration Management	Inconsistent configurations on DOI workstations	Implement least privilege principle and control the use of elevated user rights	OPEN Some DOI organizations, such as (b) (7)(E) , continue to permit users (b) (7)(E) such as local (b) (7)(E)
8.	Security Configuration Management	Disparate web browsers and unapproved FDCC deviations	Standardize Web browsers and firewalls on workstations Department- wide	OPEN There is no Departmental standard for Web browsers. There continues to be multiple web browsers in use on workstations across the Department.
9.	Security Configuration Management	DOI configuration policy needs to address all operating systems and applications across the agency, e.g. users who have administrator rights to download P2P applications, games, unauthorized software	Document and approve all deviations from FDCC compliance	OPEN There is no consistent DOI policy for the approval of FDCC deviations. Although some Bureaus/Offices permit few or no deviations from the FDCC standards (e.g. OST), other DOI organizations, such as USGS, approve thousands of deviations on a user by user basis, and others, such as FWS

No.	IT Security Program Areas	Deficiencies	Recommendations	Disposition
				widely permit user installation of 3 rd -party software.
10.	Security Configuration Management	Network access control is not deployed to prevent unauthorized computers from connecting to the network	Implement network access controls	OPEN Network Access Control (NAC) is not implemented consistently across the Department. USGS, BIA, FWS and other Bureaus/Office have generally implemented it at larger facilities, but many facilities still do not have a NAC capability.
11.	Incident Response and Reporting	Some Bureaus have their own incident response policies and procedures	Implement incident response policies and procedures consistently throughout Bureaus and Offices	OPEN Bureaus and Offices continue to have internal procedures and policies for responding to incidents that are not fully consistent with those developed for Department-wide use.
12.	Incident Response and Reporting	Lacking a Bureau- wide consolidated approach, reported incidents are not collected in a central location within DOI,	Require Bureaus and Offices to use the Department-DOI's centralized database for incident response and reporting versus their own implementation	OPEN Bureaus and Offices continue to have internal procedures and policies for responding to incidents that are not fully consistent with those developed for Department-wide use.
13.	Security Training	Supporting documentation cannot be uploaded into a system as evidence of self-certifications. Personnel with significant IT security duties that have completed role-based security training can manually self certify that they have finished	Implement a solution that assists in establishing accurate employee and contractor baseline counts, such as a central authoritative identity management system.	OPEN (NIST 800-53 Rev 3 does not include controls that could have been tested to address this prior year deficiency)
14.	Security Training	IT Security is performed by a number of personnel with an appropriate grade structure and expertise, but the results may not reveal a great deal of consistency across DOI	Review the qualifications of personnel performing IT security duties in the Department and reassign those duties accordingly.	OPEN (NIST 800-53 Rev 3 does not provide controls criteria to test the link between the overall health of the security program and organizational structure and security training of the personnel with security roles)
15.	Plan of Action and Milestone	Bureaus are gathering information in (b) (7)(E) but are not fully using it to manage IT weaknesses, manage risks, or prioritize	Ensure that the Department and Bureaus are accountable for consistent and accurate data in (b) (f)(e) to manage Plan of Action and	OPEN POA&Ms were not being effectively used to manage and remediate weakness in various Bureaus, such as BIA, BLM, BOR, FWS and NBC.

No.	IT Security Program Areas	Deficiencies	Recommendations	Disposition
		corrective action or resource allocation. The data may not be used to perform effective management and oversight of POA&M	Milestones weaknesses	Milestone remediation dates were frequently missed.
16.	Plan of Action and Milestone	Each Bureau was maintaining individual program-level POA&Ms.	Establish a senior agency information security Officer who develops and maintains an agency wide information security program required by FISMA	CLOSED DOI policy requires all POA&Ms to be entered into and maintained in b)(7)(E) and reported to OCIO on a quarterly basis. This requirement met across DOI.
17.	Remote Access	Bureaus maintain and use separate remote access systems	Consolidate remote access solutions to allow efficiency and reduce duplicative services	OPEN While all Bureaus and Offices are required to use the (b) (7)(E) some are still using their own solutions.
18.	Remote Access	DOI does not enforce two-factor authentication for remote services because not all personnel have been issued PIV cards	Enforce two-factor authentication	OPEN DOI has taken steps to enforce the use of 2-factor authentication, but those steps have not yet been implemented. DOI memorandum "Policy for the Issuance, Management and Use of Federal Personal Identity Verification (PIV) Cards (DOI Access Cards)" dated March 31, 2011 prescribes the policy to necessary to expedite full deployment and use of PIV credentials (DOI Access Cards) as the common means of authentication for access to facilities, networks, and information systems within the DOI. The beginning of FY2012 and in accordance with HSPD-12 and NIST guidelines, existing physical and logical access control systems must be upgraded to use the DOI Access Card prior to the agency using development and technology refresh funds to complete other activities.

No.	IT Security Program Areas	Deficiencies	Recommendations	Disposition
19.	Remote Access	Not able to validate that personal computers are configured securely with the proper security configuration to connect remotely	Enable host checking for remote access	OPEN The Department does not yet implemented the capability for checking to validate that personal computers are configured securely.
20.	Remote Access	Lack of telework or remote access policy addressed within the Rules of Behavior from Bureaus	Update the telework policy to reflect the implementation of NIST 800-46 Rev 1, "Guide to Enterprise Telework and Remote Access Security"	OPEN Various Bureaus, such as USGS, have not established telework or remote access policies that make the use of Government Furnished Equipment (GFE) mandatory, and have not established mandatory security requirements for the use of non- GFE equipment.
21.	Account and Identity Management	Poor account management practices; e.g. procedures for changing passwords are not followed	Ensure account management procedures adhere to policies	OPEN We did not observe a DOI-wide process for validating that a (b) (7)(E) requirement is implemented as required by the (b) (7)(E).
22.	Account and Identity Management	Inadequate procedures to validate users password changes	Ensure identity verification security questions are unique and answers cannot be easily obtained	OPEN We did not observe a DOI-wide process for validating that users change their password as required by the (b) (7)(6).
23.	Account and Identity Management	PIV cards are not issued agency wide, employing a two factor authentication, granting users access when combining PIV card and password or personal identification number	Issue PIV cards to all employees and contractors	OPEN DOI has taken steps to enforce the use of 2-factor authentication, but those steps have not yet been implemented. DOI memorandum "Policy for the Issuance, Management and Use of Federal Personal Identity Verification (PIV) Cards (DOI Access Cards)" dated March 31, 2011 prescribes the policy to necessary to expedite full deployment and use of PIV credentials (DOI Access Cards) as the common means of authentication for access to facilities, networks, and information systems within the DOI. The beginning of FY2012 and in accordance with HSPD-12 and NIST guidelines, existing physical and logical access control systems must be upgraded to use the DOI Access Card prior to the agency using

No.	IT Security Program Areas	Deficiencies	Recommendations	Disposition
				development and technology refresh funds to complete other activities.
24.	Account and Identity Management	PIV cards are not enforced to confirm users' identities to increase IT security	Enforce the use of PIV cards for all employees and contractors	OPEN DOI has taken steps to enforce the use of 2-factor authentication, but those steps have not yet been implemented. DOI memorandum "Policy for the Issuance, Management and Use of Federal Personal Identity Verification (PIV) Cards (DOI Access Cards)" dated March 31, 2011 prescribes the policy to necessary to expedite full deployment and use of PIV credentials (DOI Access Cards) as the common means of authentication for access to facilities, networks, and information systems within the DOI. The beginning of FY2012 and in accordance with HSPD-12 and NIST guidelines, existing physical and logical access control systems must be upgraded to use the DOI Access Card prior to the agency using development and technology refresh funds to complete other activities.
25.	Continuous Monitoring	Lacking enterprise- wide strategy to develop continuous monitoring policies	Create a comprehensive, enterprise-wide strategy for continuous monitoring	OPEN Although DOI has elements of a continuous monitoring strategy in place, such as the requirement for annual Internal Control Reviews (ICR), it has not established and overall Risk Management Framework that identifies the roles, responsibilities and procedures at all levels of the DOI hierarchy for continuous monitoring, risk assessment and reporting.

No.	IT Security Program Areas	Deficiencies	Recommendations	Disposition
26.	Continuous Monitoring	Ongoing results from continuous monitoring, updated security plans, security assessment reports, and POAMs are not reported regularly and may need guidance on format and content	Establish a format and content template for the authorizing official's security status reports	OPEN Although DOI has elements of a continuous monitoring strategy in place, such as the requirement for annual Internal Control Reviews, it has not established and overall Risk Management Framework that identifies the roles, responsibilities and procedures at all levels of the DOI hierarchy for continuous monitoring, risk assessment and reporting.
27.	Continuous Monitoring	Processes have not been completed to enable network adjustments for IT assets to detect changes in the network infrastructure	Enhance the Department's continuous monitoring program using existing investments	OS/ISD monitors all changes to the DOI network on a daily basis using (b) (7)(E) tool.
28.	Continuous Monitoring	Multitude of automated capabilities for continuous monitoring, are not fully implemented to integrate data feeds	Ensure that Bureaus are reporting to centralized Departmental continuous monitoring systems	OPEN Although DOI has elements of a continuous monitoring strategy in place, such as the requirement for annual Internal Control Reviews (ICR), it has not established and overall Risk Management Framework that identifies the roles, responsibilities and procedures at all levels of the DOI hierarchy for continuous monitoring, risk assessment and reporting. In addition, the capability does not yet exist for integrated, Department-wide automated reporting of near real time information for technical and management consideration of risk.
29.	Contingency Planning	Contingency plans are not documented properly or annually updated and tested in accordance with NIST SP 800-34 Rev 1, Contingency Planning Guide for Information Technology Systems	Update contingency planning guidance to correspond with NIST SP 800-34 Rev 1, Contingency Planning Guide for Information Technology Systems	OPEN. Not all system specific contingency plans had annual testing performed.

No.	IT Security Program Areas	Deficiencies	Recommendations	Disposition
30.	Contingency Planning	The effectiveness of the DOI policy, Continuity of Operations Plan (COOP) was not tested and results were not adequately documented	Update the DOI policy, COOP to reflect changes to the scope, establish objectives of the test, update contact information, add lessons learned and results	OPEN Implementation of continuity planning policies is inconsistent across the Department. Not all systems had alternative processing sites, tests are not conducted regularly, and results are not always used to make improvements.
31.	Oversight of Contract Systems	Policies are not updated to reflect oversight of contractor roles and responsibilities, and involvement in the C&A process	Define, document, and establish procedures for contactor oversight in accordance with FISMA requirements	OPEN DOI does not yet have adequate policies and procedures for information security oversight of systems operated on the Department's behalf by contractors and other entities.
32.	Oversight of Contract Systems	IT Security requirements are not being consistently included in IT service contracts	Coordinate between IT security and the associated procurement contracting Office	OPEN. DOI does not yet have adequate policies and procedures for information security oversight of systems operated on the Department's behalf by contractors and other entities.

APPENDIX III – 2011 CYBERSCOPE FISMA QUESTIONNAIRE RESPONSES

The following tables contain our responses to the control metrics established by DHS for the annual OIG FISMA Questionnaire (CyberScope) and the 2011 OMB FISMA reporting guidance in memorandum M-11-33. Each question can have one out of three possible responses. Response "a" indicates, "The Agency has established and is maintaining a program [for that control metric] that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines." Response "b" indicates, "The Agency has established and is maintaining a program [for that control metric]. However, the Agency needs to make significant improvements." Response "c" indicates that there is no program and was not selected for any control metric in regards to DOI. When either "a" or "b" is selected (i.e., a "Yes" response) on CyberScope, the tool will then present the relevant sub questions. Comments were only provided for the sub-questions under "a" or "b" would be visible on CyberScope. The meaning of "Yes" and "No" in the table below depends on the question and we used the narrative to clarify the meaning of each response.

1.	Risk Management	Response	Comments
	Questions	Yes/No	Comments
1.a	The Agency has established and is maintaining a Risk Management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No	
1.b	The Agency has established and is maintaining a risk management program. However, the Agency needs to make significant improvements as noted below.	Yes	
1.b(1)	Risk Management policy is not fully developed.	Yes	Yes, improvements are needed. NIST SP 800-37, Revision 1, February 2010 transforms the "security authorization process" by incorporating system risks, mission risks and organizational risks into a Risk Management Framework (RMF) that puts the evaluation of system risk into a broader context, and emphasizes the continuous awareness of risks and of the security state of the system. Although various DOI policies have elements, which could support this updated approach, they have not yet been integrated into a cohesive RMF for DOI. The DOI (b) (7)(E) (b) (7)(E) has not been updated to incorporate NIST SP 800-37 Revision 1. The

1.	Risk Management	Response		
	Questions	Yes/No	Comments	
			identifies a hierarchy of roles and responsibilities that are involved with the assessment of system, mission, and organizational risks, but does not provide an overall strategy, plan, and process for IT governance and risk management.	
1.b(2)	Risk Management procedures are not fully developed, sufficiently detailed (SP 800-37, SP 800-39, SP 800-53).	Yes	Yes, improvements are needed. OCIO Directive 2009-04 "Internal Control Review (ICR) Guidance for Fiscal Year (FY) 2009" and "FY10 DOI Information Technology (IT) Systems Renewal and Certification and Accreditation (C&A) Guidance," June 3, 2010, provide elements that seem to fit RMF continuous monitoring concepts by establishing an annual process for assessing system controls in accordance with NIST SP 800-53 Revision 3 on a 3-year cycle, and suspending the previous practice of assessing 100% of the security control baselines every year. OCIO Directive 2010-009 July 7, 2010 "Risk Management Framework – Delegation of Authorizing Officials and Bureau/Office Continuous Monitoring Process" also has elements concerning the types and use of automated tools that are needed to support continuous monitoring. However, the Department has not yet laid out a strategy, plan, and procedures for integrating and implementing all the elements of an RMF.	
1.b(3)	Risk Management procedures are not consistently implemented in accordance with government policies (SP 800-37, SP 800-39, and SP 800-53).	Yes	Yes, improvements are needed. The DOI (b) (7)(E) (b) (7)(E) has not been updated to incorporate NIST SP 800- 37 Revision 1 guidance. Although various DOI policies have elements that conform to the updated NIST Risk Management Framework (RMF), they have not yet been integrated into a cohesive document. Security documentation is recorded inconsistently on the (b) (7)(E) (b) (7)(E) DOI risk management procedures should provide clarity to the bureaus/offices on how to record the RMF documentation consistently on (b) (7)(E) since inconsistent records make it harder to track the completion of risk management activities and assess the quality of the information available.	
1.b(4)	A comprehensive governance structure and Agency-wide risk management strategy has not been fully developed in accordance with government policies (SP 800-37, SP 800-39, SP	Yes	Yes, improvements are needed. The DOI (b) (7)(E) (b) (7)(E) has not been updated to incorporate NIST SP 800-37 Revision 1 guidance. Although the identifies a hierarchy of roles and responsibilities that are involved with the assessment of business process and mission risks, it does not provide a risk management governance structure and process, nor provide for a Department-wide risk management strategy and	

1.	Risk Management	Response	
	Questions	Yes/No	Comments
	800-53).		implementation plan.
1.b(5)	Risks from a mission and business process perspective are not addressed (SP 800-37, SP 800-39, SP 800-53)	Yes	Yes, improvements are needed. NIST SP 800-37, Revision 1, February 2010 transforms the "security authorization process" by incorporating system risks, mission risks and organizational risks into a Risk Management Framework (RMF) that puts the evaluation of system risk into a broader context, and emphasizes the continuous awareness of risks and of the security state of the system. Although various DOI policies have elements that could support this updated approach, they have not yet been integrated into a cohesive RMF for DOI. The DOI (b) (7)(E) has not been updated to incorporate NIST SP 800-37 Revision 1. The (b) (7)(E) identifies a hierarchy of roles and responsibilities that are involved with the assessment of system, mission, and organizational risks, but does not provide an overall strategy, plan, and process for IT governance and risk management.
1.b(6)	Information systems are not properly categorized (FIPS 199/SP 800-60).	No	No improvements are needed. Our sample of system at 12 bureaus/offices included systems with a mix of high, moderate, and low impact systems. Inspection of the System Security Plans (SSP) for all the systems within scope indicates the FIPS 199/ NIST 800-60 categorization process was followed and documented appropriately.
1.b(7)	Appropriately tailored baseline security controls are not applied to information systems in accordance with government policies (FIPS 200/SP 800-53).	Yes	Yes, improvements are needed. Security control baselines are not tailored to individual systems. One reason for the lack of tailoring is that some bureaus are relying on for the generation and maintenance of System Security Plans (SSP), but the controls documented in the system Security Plans (SSP), but the controls documented in the system of SSPs are exact copies of NIST 800-53, Revision 3 controls and do not allow controls to be tailored. At present, some does not permit direct entry of information about how controls are implemented and instead uses the results of ICR testing to populate the SSP controls fields. Although this approach provides consistency, it appears to have significantly reduced the level of detail available on the actual implementation of controls.
1.b(8)	Risk assessments are not conducted in accordance with government policies (SP 800-37, SP 800-30).	Yes	Yes, improvements are needed. The DOI (b) (7)(E) (b) (7)(E) has not been updated to incorporate NIST 800-53 Revision 3 guidance, which updates the security control baselines that should be used for the various system categories and form the basis for risk assessments. Although the (b) (7)(E)

1.	Risk Management Response		
	Questions	Yes/No	Comments
			tool was updated this year with the new control sets, not all risk assessments have been updated yet either manually or on (b) (7)(=
1.b(9)	Security control baselines are not appropriately tailored to individual information systems in accordance with government policies (SP 800-53).	Yes	Yes, improvements are needed. Security control baselines are not tailored to individual systems. The controls documented in the generated System Security Plans (SSPs) are exact copies of NIST 800-53, Revision 3 controls.
1.b(10)	The communication of information system specific risks, mission/business specific risks and organizational level (strategic) risks to appropriate levels of the organization is not in accordance with government policies.	Yes	Yes, improvements are needed. The DOI (b) (7)(E) (b) (7)(E) has not been updated to incorporate NIST SP 800- 37 Revision 1 guidance. Although it identifies a hierarchy of roles and responsibilities that are involved with the assessment of business process and mission risks, it does not provide an RMF governance structure and process, nor provide for a Department-wide risk management strategy.
1.b(11)	The process to assess security control effectiveness is not in accordance with government policies (SP800 53 A).	Yes	Yes, improvements are needed. The Department has issued guidance that provides for the assessment of NIST SP 800-53 Revision 3 controls and the re-authorization of systems that is in line with continuous monitoring guidance in NIST SP 800-37 Revision 1. However, it has not provided guidance for the risk management aspects of SP 800-37 Revision 1, except that which existed in the previous version for system level risks.
1.b(12)	The process to determine risk to agency operations, agency assets, or individuals, or to authorize information systems to operate is not in accordance with government policies (SP 800-37).	Yes	Yes, improvements are needed. The DOI (b) (7)(E) has not been updated to incorporate NIST SP 800- 37 Revision 1 guidance. Although it identifies a hierarchy of roles and responsibilities that are involved with the assessment of business process and mission risks, it does not provide an RMF governance structure and process, nor provide for a Department-wide risk management strategy, plans and process. Because DOI guidance for conducting risk assessment has not been updated, risk assessments are not conducted in accordance with government policies. There is no Department-wide risk executive function.
1.b(13)	The process to continuously monitor	Yes	Yes, improvements are needed. The Department has issued some guidance that is in line with NIST SP 800-37 Revision

1.	Risk Management	Response	
	Questions	Yes/No	Comments
	changes to information systems that may necessitate reassessment of control effectiveness is not in accordance with government policies (SP 800-37).		1 processes for continuous monitoring. "FY10 DOI Information Technology (IT) Systems Renewal and Certification and Accreditation (C&A) Guidance," June 3, 2010 provides guidance on the Internal Control Review (ICR) process for annual self-assessments of security controls across the Department and satisfies NIST SP 800-53 Revision 3 and SP 800-37 Revision 1 requirements for the reauthorization of systems. OCIO Directive 2010-009 July 2, 2010 addresses the types and use of automated tools that are needed to support continuous monitoring in Appendix 2. However, the Department has not yet laid out a strategy, plan and process for integrating and implementing all the elements of an RMF.
1.b(14)	Security plan is not in accordance with government policies (SP 800-18, SP 800-37).	No	No improvements are necessary. All the Security Plans reviewed followed NIST SP 800-18.
1.b(15)	Security assessment report is not in accordance with government policies (SP 800-53A, SP 800-37).	No	No improvements are needed. DOI established an Internal Control Review (ICR) process to conduct annual self-assessments of security controls across the Department. The Department specifies which controls are to be tested in the current year. Because of their nature some controls are tested every year, while others may be tested only once in a 3 year period. At the end of a 3-year cycle, all SP 800-53 controls would have been tested. All controls testing results are recorded in (b) (7)(E) is capable of producing reports of test results from the ICR data entered. This process is consistent with NIST SP 800-37 Revision 1 and 800-53 Revision 3.
1.b(16)	Accreditation boundaries for agency information systems are not defined in accordance with government policies.	Yes	Yes, improvements are needed. While most of the systems in our test sample had accurately documented their accreditation boundary in their System Security Plans, some systems did not identify the minor applications within their boundary as a "FISMA Child" in the (b) (7)(E) system. In addition, several systems identified within (b) (7)(E) are used to group loosely related systems that should otherwise be recorded separately because they do not share controls. In other instances, systems are lumped together under a common name/boundary in (b) (7)(E) but the system security plans are either incomplete or address only a single system or geographical area without providing equivalent security controls information for the remaining systems or areas.

2.	Configuration Management	Response	Comments
	Questions	Yes/No	
2.a	The Agency has established and is maintaining a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No	
2.b	The Agency has established and is maintaining a security configuration management program. However, the Agency needs to make significant improvements as noted below.	Yes	
2.b(1)	Configuration management policy is not fully developed (NIST 800-53: CM-1)	No	No improvements are needed. The (b) (7)(E) address configuration management policy.
2.b.(2)	Configuration management procedures are not fully developed (NIST 800-53:CM-1)	Yes	Yes, improvements are needed. Configuration management procedures are not fully developed. The procedures do not fully address handling legacy systems and establishing baselines for third party applications.
2.b(3)	Configuration management procedures are not consistently implemented (NIST 800-53:CM-1)	Yes	Yes, improvements are needed. The Department has not defined uniform configuration management procedures and therefore some bureaus have implemented their own procedures resulting in configuration management inconsistencies across the bureaus. We noted that deficiencies such as failure to limit the number of deviations, approving or rejecting deviations, and longstanding POA&Ms for eliminating unapproved deviations.
2.b(4)	Standard baseline configurations are not identified for software components (NIST 800-	Yes	Yes, improvements are needed. The Department's bureaus/offices have generally developed baseline configuration standards for Windows based systems. However, bureaus have individually decided how to tailor the baselines and what range of deviations to permit. In some

2.	Configuration Management	Response	Comments
	Questions	Yes/No	
	53: CM-2).		instances (e.g., USGS), the bureaus have accepted deviations that vary from system to system. Baselines for other types of operating systems have been developed to a lesser extent. Even when baselines exist, bureaus/offices with (b) (7)(E) (b) (7)(E) generally permit local tailoring of the security configuration. We did not identify baseline configurations for all third-party software.
2.b(5)	Standard baseline configurations are not identified for all hardware components (NIST 800-53: CM-2).	Yes	Although standard baseline configurations are available for the most current and/or prevalent types of hardware, baseline configurations are frequently not available for less prevalent and older hardware installations and third party software such as (b) (7)(E)
2.b(6)	Standard baseline configurations are not fully implemented (NIST 800-53: CM-2).	Yes	Yes, improvements are needed. Bureaus/offices such as OST and BIA have implemented automated reporting to (b) (7)(E) even though the Department has not yet implemented a standard compliant hardware detection and inventory tool. Implementation of baseline configurations for (b) (7)(E) is more consistent across the Department than baseline configurations for variations of (b) (7)(E)
2.b(7)	FDCC/USGCB is not fully implemented (OMB) and/or all deviations are not fully documented (NIST 800- 53:CM-6)	Yes	Yes, improvements are needed. Bureaus/Offices have deployed (b) (7)(E) security configurations with deviations to their workstations, but the processes for approving deviations and reporting compliance differ so much between bureaus/offices that it could not be determined to what extent the Department as a whole is in compliance. In general, each bureau/office has processes for approving deviations. However, those processes vary from permitting only deviations that are standard for the entire bureau to permitting workstation by workstation deviations. DOI lacks of specific guidance and criteria for what constitutes compliance, how to scan consistently for it, and how to report compliance scan results. As a result, reporting is currently decentralized with bureaus/offices applying separate interpretations of what constitutes compliance.
2.b(8)	Software assessing	Yes	Yes, improvements are needed. We also found various

2.	Configuration Management	Response	Comments
	Questions	Yes/No	
	(scanning) capabilities are not fully implemented (NIST 800-53: RA-5, SI-2).		scanning capabilities implemented throughout 11 of the 12 bureaus/offices. However, a variety of products is in use and produce outputs that can be difficult to correlate. There is no Departmental guidance on the implementation of these tools and therefore some bureaus/offices are not taking full advantage of their capabilities. While some bureaus/offices monitor the output of their automated systems very closely, others have a more ad hoc approach and not all systems are regularly scanned. We did not learn of any instances of specialized scanning of in-house developed software.
2.b(9)	Configuration-related vulnerabilities, including scan findings, have not been remediated in a timely manner, as specified in Agency policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2).	Yes	Yes, improvement is needed. (See 2.b(10) for related comments.) We looked at patch management processes for remediating vulnerabilities in both Operating System and third-party applications. We found most Bureaus/Offices were remediating scan findings on Operating Systems in a timely manner, but 3 out of 12 Bureaus/Offices were not timely with OS patching. For third-party applications, 10 out of 12 Bureaus/Offices were not remediating those applications in a timely manner, primarily because of the manual nature of the remediation and the lower priority given to such patches by system administrators.
2.b(10)	Patch management process is not fully developed, as specified in agency policy or standards. (NIST 800-53: CM-3, SI-2).	Yes	Yes, needs improvement. Bureau/Office vulnerability management processes ranged from organized and mature to ad-hoc. We looked at patch management processes for remediating vulnerabilities in both Operating System (OS) and third party applications. We found that 11 out of 12 bureaus/offices had one or more weaknesses and all bureaus had high risk vulnerabilities DOI has not issued consistent guidance to the bureaus/offices on the use of vulnerability scanning tools. While bureaus typically use similar scanning tools that could report on software patching issues, they were not typically configured to scan with enough permissions. Vulnerabilities identified through scans at 5 bureaus were often left unmitigated for at least 5 months. Bureaus/Offices gave priority to OS patches over 3rd-party application patches and often did not track the 3rd-party application issues. Tools to handle the third-party application

3.	Incident Response	Response	
	Questions	Yes/No	Comments
3.a	The Agency has established and is maintaining an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No	
3.b	The Agency has established and is maintaining an incident response and reporting program. However, the Agency needs to make significant improvements as noted below:	Yes	
3.b(1)	Incident response and reporting policy is not fully developed (NIST 800-53: IR-1)	No	No improvements needed. Although some bureaus/offices have additional incident response policies and guidelines, they generally adhere to the DOI IT Security Policy Handbook.
3.b(2)	Incident response and reporting procedures are not fully developed or sufficiently detailed (NIST 800-53: IR-1)	Yes	Yes, improvements are needed. The DOI Computer Security Incident Response Handbook, v2.2.9 dated April 21, 2010 provides response and reporting procedures for the bureaus/offices, but we found it was not implemented consistently. Some bureaus/offices have incident response procedures tailored to their own environments, while others appear to fully implement the Handbook procedures. There is no consistent guidance on how to make reports to DOI-CIRC and the level of detail provided varies greatly from one incident report to the other.
3.b(3)	Incident response and reporting procedures are not consistently implemented in accordance with government policies (NIST 800-61, Rev1).	Yes	Yes, improvements are needed. Because some Bureaus have incident response procedures tailored to their own operations the implementation of such procedures is likely to vary significantly from other Bureaus. The weakest link appears to be individual employees that might interpret the procedures differently depending on the circumstances. DOI does have common procedures for reporting to CIRC, but we noted that the level of detail in those reports varies

3.	Incident Response	Response	
	Questions	Yes/No	Comments
			significantly.
3.b(4)	Incidents were not identified in a timely manner, as specified in agency policy or standards (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).	Yes	Yes, improvements are needed. While incident reporting is completed within the required timeframes once it is captured by a reporting mechanism, incidents detected by individuals are not being reported consistently within the required timeframe. Once the incident is captured, a DOI CIRC ticket is created with the option to report to the US-CERT and law enforcement when necessary.
3.b(5)	Incidents were not reported to US-CERT as required (NIST 800-53, 800-61, and OMB M-07- 16, M-06-19).	No	No improvements needed. When the bureaus report to the DOI Computer Incident Response Center the individual making the report can request that a report be automatically forwarded to the US Computer Emergency Response Team as required by the Computer Incident Response Handbook for the type of incident.
3.b(6)	Incidents were not reported to law enforcement as required (SP 800-86).	No	No improvements needed. At the Department level, incidents that need to be reported to Law Enforcement are reported automatically once the information makes it to DOI Computer Incident Response Center and US Computer Emergency Response Team. Some bureaus/offices indicated they report these incidents directly to the OIG Computer Crimes Unit.
3.b(7)	Incidents were not resolved in a timely manner (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).	No	No improvements needed. We reviewed a sample of incidents and determined their resolution adhered to the timeframes for reporting incidents by category in the Computer Security Incident Response Handbook.
3.b(8)	Incidents were not resolved to minimize further damage (NIST 800-53, 800-61, and OMB M-07-16, M-06-19).	No	No improvements are needed. All the incidents in our sample were reported and resolved within the required timeframes.
3.b(9)	There is insufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61,	No	No improvements are needed (b) (7)(E) (b) (7)(E) provides Department-wide external boundary intrusion detection.

3.	Incident Response Questions	Response Yes/No	Comments
	and OMB M-07-16, M-06-19).		
3.b(10)	The agency cannot or is not prepared to track and manage incidents in a virtual/cloud environment.	Yes	Yes, improvements are needed. DOI does not currently implement a virtual/cloud architecture or uses services from a public cloud. To track and manage incidents in a cloud environment, DOI might need to add contract requirements and implement tools to obtain external incident reports from the cloud provider.
3.b(11)	The agency does not have the technical capability to correlate incident events.	Yes	Yes, improvements are needed. DOI has not implemented a (b) (7)(E) solution to improve its technical capability to gather, correlate, report, and retain incident event information.

4.	Cyber Security Training	Response	Community
	Questions	Yes/No	Comments
4.a	The Agency has established and is maintaining a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.	Yes	
4.a(1)	Documented policies and procedures for security awareness training.	Yes	No improvements are needed. The DOI (b) (7)(E) (b) (7)(E) documents policies requiring annual security training and awareness. DOI personnel are enrolled in required annual FISSA training and users are notified by email generated by the DOI Learn, the Department-wide training system.
4.a.(2)	Documented policies and procedures for specialized training for users with significant information security responsibilities.	Yes	No improvements are needed. DOI has documented policies and procedures addressing specialized training for users with significant information security responsibilities. Role Based Security Training standards are detailed in the Role Based Security Training Standard v2.6.0 (March 11, 2011) and that cover all individuals with significant cyber security responsibilities. DOI uses the Department-wide training system,
4.a.(3)	Security training content based on the organization and roles, as specified in agency policy or standards.	Yes	No improvements are needed. DOI uses a Department-wide training system, DOI Learn, which tracks individuals requiring specialized cyber security training based on their job functions and roles. It is the responsibility of employees and their supervisor, contractor and contract management staff, and the Bureau/Office CISO to ensure that the employee/contractor has sufficient role based security training to adequately fulfill the information security responsibilities of his/her assigned role. Individuals are notified annually of their specific cyber security training requirements and provided information on recommended training that meets their specialized training requirements.
4.a.(4)	Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other agency users) with access privileges that require security awareness training.	Yes	No improvements are needed. DOI personnel are enrolled in required annual FISSA training and users are notified by email generated by the DOI Learn, the Department-wide training system. DOI Learn is also used to track the completion of the required training, and notifies individuals and management when the required training deadlines are not met. It is the responsibility of employees and their supervisor, contractor and contract management staff, and the Bureau/Office CISO to ensure that the employee/contractor has met security training requirements.
4.a(5)	Identification and tracking of the status of specialized training for all personnel (including	Yes	No improvements are needed. DOI uses a Department-wide training system, DOI Learn, to track individuals requiring specialized cyber security training based on their job functions and roles. It is the responsibility of employees and

4.	Cyber Security Training	Response	Comments
	Questions	Yes/No	Comments
	employees, contractors, and other agency users) with significant information security responsibilities that require specialized training.		their supervisor, contractor and contract management staff, and the Bureau/Office CISO to ensure that the employee/contractor has sufficient role based security training to adequately fulfill their information security responsibilities. Individuals are notified annually of their specific cyber security training requirements and provided information on recommended training that meets their specialized training requirements.

5.	POA&M	Response	
	Questions	Yes/No	Comments
5.a.	The Agency has established and is maintaining a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses?	No	
5.b	The Agency has established and is maintaining a POA&M program that tracks and remediates known information security weaknesses. However, the Agency needs to make significant improvements as noted below	Yes	
5.b(1)	POA&M Policy is not fully developed.	No	No improvements are needed. The DOI (b) (7)(E) (b) (7)(E) states bureaus/offices "shall develop and ensure the continuous update of a plan of action and milestones (POA&M) for all information systems that fully documents their organization's planned, implemented, and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system in accordance with the DOI POA&M Process Standard." This policy was reiterated in OCIO Directive 2010-006 on May 18, 2010. An updated version of the DOI POAM Process Standard, (b) (7)(E)
5.b(2)	POA&M procedures are not fully developed and sufficiently detailed.	Yes	Yes, improvements are needed. DOI's documented POA&M procedures comply with OMB M-04-25. The DOI POA&M Process Standard, version 1.8, dated May 10, 2010 incorporates procedures for the use of (b) (7)(E) for automating the process. Nevertheless, the procedures outline

5.	POA&M	Response	
	Questions	Yes/No	Comments
			considerations regarding the prioritization of corrective actions, but lack specificity regarding the process for managing the assignment of resources based on risk related priorities and resource constraints.
5.b(3)	POA&M procedures are not consistently implemented in accordance with government policies.	Yes	Yes, improvements are needed. Although most bureaus/offices implemented the DOI POA&M Process Standard, they failed to identify the source of the findings addressed by the POA&Ms as required by the Process Standard. A lead reason is that, the (b) (7)(E) does not have a specific box for identifying the source of the finding addressed in the POA&M and therefore this information is often not recorded.
5.b(4)	POA&Ms do not include security weaknesses discovered during assessments of security controls and requiring remediation. (OMB M-04-25).	No	No improvements are needed. We found that security weaknesses discovered during assessments of security controls were included in the POA&M reviewed for each Bureau as required by the Process Standard. All the bureaus/offices follow the DOI POA&M Process Standard, which requires the use of to track the POA&Ms.
5.b(5)	Remediation actions do not sufficiently address weaknesses in accordance with government policies (NIST SP 800-53, Rev. 3, Section 3.4 Monitoring Security Controls).	No	No improvements needed. The POA&Ms reviewed appeared to sufficiently address the findings they were intended to remediate.
5.b(6)	Source of security weaknesses are not tracked (OMB M-04-25).	Yes	Yes, improvements are needed. Although the procedures in the POA&M Process Standard require the tracking of the source of all POA&Ms, we found this was not been done consistently. We also noted the (a) (7)(E) did not have a specific box to enter this information, therefore for a Bureau to comply they have to come up with their own guidance on how to record the source of the finding being addressed resulting in inconsistent tracking.
5.b(7)	Security weaknesses are not appropriately prioritized (OMB M-04-25).	Yes	Yes, improvements are needed. Prioritization is done on at the system level by assigning criticality to the severity of the finding. Without considering Return on Investment (ROI) and costs, criticality alone does not

5.	POA&M	Response	
	Questions	Yes/No	Comments
			translate into proper ranking of priorities at the system level or at the Bureau level and might be a factor leading to problems missing completion deadlines.
5.b(8)	Milestone dates are not adhered to. (OMB M-04-25).	Yes	Yes, improvements are needed. We found that at milestone dates are frequently not adhered to. The reasons for this appear to be misunderstanding of the POA&M process, lack of clear delineation of accountability, or lack of uniform procedures and tools for prioritizing corrective action in a way that takes in consideration both the criticality of the issues, return on investment, and resource availability. We observed that POA&M items are often assigned to the same person or not assigned at all and this may account for missed milestones.
5.b(9)	Initial target remediation dates are frequently missed (OMB M-04-25).	Yes	Yes, improvements are needed. We found that milestone dates are frequently not adhered to. We observed this deficiency at 5 bureaus. For example, at one bureau several items were listed with a planned finish that was moved without a corresponding adjustment to the milestone dates.
			The reasons for this appear to be misunderstanding of the POA&M process, lack of clear delineation of accountability, or lack of uniform procedures and tools for prioritizing corrective action in a way that takes in consideration both the criticality of the issues, return on investment, and resource availability.
5.b(10)	POA&Ms are not updated in a timely manner (NIST SP 800- 53, Rev. 3, Control CA- 5, and OMB M-04-25).	Yes	Yes, improvements are needed. The DOI POA&M Process Standard requires that POA&Ms be reviewed and updated at least quarterly. However, some bureaus/offices do not appear to update their POA&Ms consistently. For example, at one bureau several items were listed as status pending with little or no recent updates, indicating that the item has not been reviewed quarterly in accordance with policy.
5.b(11)	Costs associated with remediating weaknesses are not identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25).	Yes	Yes, improvements are needed. We found that the estimated remediation costs were not always associated with POA&M weaknesses. For example at one bureau, costs of fixes are not being accurately recorded and all items reviewed listed a cost of \$10,000. At another bureau, costs were not tracked at all.

5.	POA&M	Response	Comments
	Questions	Yes/No	
5.b(12)	Agency CIO does not track and review POA&Ms (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25).	No	No improvements are needed. The DOI POA&M Process Standard requires the bureaus to review, update, and sent POA&Ms to the DOI CIO at least quarterly. The Department provided evidence of the quarterly POA&M updates according to policy.

6.	Remote Access	Response	
	Questions	Yes/No	Comments
6.a	The Agency has established and is maintaining a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No	
6.b	The Agency has established and is maintaining a remote access program. However, the agency needs to make significant Improvements as noted below.	Yes	
6.b(1)	Remote access policy is not fully developed (NIST 800-53: AC-1 and AC-17).	No	No improvements needed. The DOI (b) (7)(E) (b) (7)(E) and augmenting OCIO policy memoranda establish policies that adequately meet the NIST SP-800-53 requirements of AC-1 and AC-17.
6.b(2)	Remote access procedures are not fully developed and sufficiently detailed (NIST 800-53: AC-1 and AC-17).	Yes	Yes, improvements are needed. Most DOI bureaus/offices are using the Department's remote access service to establish virtual private network (VPN) connections. However, two modes of authentication are permitted, 1) using a PIV card or 2) using only userid and password. The userid and password mode does not adequately meet NIST requirements for identification and authentication.
6.b(3)	Remote access procedures are not consistently implemented in accordance with government policies (NIST 800-53: AC-1 and AC-17)	Yes	Yes, improvements are needed. At least two bureaus/offices have implemented remote access solutions other than the VPN solution required by DOI policy. In addition, the Department has allowed the individual bureaus/offices using their solution to decide whether to use of the PIV card for 2-factor authentication for remote access is mandatory. DOI implemented a waiver process for each user that does not follow the PIV requirement, but that process does not appear to be followed by every bureau/office. Most components permit remote users to use the userid/password only mode because a significant

6.	Remote Access	Response	
	Questions	Yes/No	Comments
			percentage of their remote users have not yet obtained a PIV card. Additionally, although DOI policies permit only government furnished equipment (GFE) to be used for remote access, in practice this policy is not enforced and both personal equipment and the equipment of non-federal users is permitted.
6.b(4)	Telecommuting policy is not fully developed (NIST 800-46, Section 5.1).	Yes	Yes, improvements are needed. The DOI (b) (7)(E) (b) (7)(E) and augmenting memoranda require bureaus/offices to cover the contents of telecommuting and remote access in their Rules of Behavior. However, we found that Bureau and Office Rules of Behavior did not require GFE for remote access did not require standard security configuration settings, and did not require 2-factor authentication. Additionally, the pre-conditions and requirements for permitting remote access by non-federal users are not adequately defined.
6.b(5)	Telecommuting procedures are not fully developed or sufficiently detailed in accordance with government policies (NIST 800-46, Section 5.4).	Yes	Yes, improvements are needed: We found telecommuting procedures are not fully developed within the DOI (b) (7)(E). The (b) (7)(E) requires only Federal Government and authorized hardware/software be installed at the telework location; however, we found DOI allows any home or personal computer to download the remote access client and connect to their Bureau. Furthermore, the agency does not restrict non-government equipment from participating and connecting to the enterprise via telecommuting which is in direct conflict of the (b) (7)(E)
6.b(6)	Agency cannot identify all users who require remote access (NIST 800-46, Section 4.2, and Section 5.1).	Yes	Yes, improvements are needed. The Department has not adequately defined who is eligible to utilize remote access. At present non-federal users who would not qualify for a PIV card are permitted to use remote access without defined and specific pre-conditions or requirements.
6.b(7)	Multi-factor authentication is not properly deployed (NIST 800-46, Section 2.2, Section 3.3).	Yes	Yes, improvements are needed. NIST SP 800-46 requires remote access only with two-factor authentication. In 9 of the 12 bureaus/offices reviewed there remained employees, contractors and others who require a PIV card who had not yet obtained one. Additionally, DOI has not enforced two-factor authentication for users who have the ability to use the PIV card.
6.b(8)	Agency has not identified all remote	Yes	Yes, improvements are needed. DOI relies on the bureaus/offices to identify remote devices for the users to

6.	Remote Access	Response	
	Questions	Yes/No	Comments
	devices (NIST 800-46, Section 2.1).		whom they authorize access. However, the bureaus/offices permit employees, contractors, collaborators and others to use their own equipment without ensuring that that equipment has been properly secured.
6.b(9)	Agency has not determined all remote devices and/or end user computers have been properly secured (NIST 800-46 Section 3.1 and 4.2).	Yes	Yes, improvements are needed. DOI relies on the bureaus/offices to identify the remote devices of users for whom they authorize access. However, the bureaus/offices permit employees, contractors, collaborators and others to use their own equipment without ensuring that equipment has been properly secured. The Department has authorized the connection of the DOI network. The is known to have weak, not NIST compliant encryption, does not have the capability to use the PIV card for authentication, and information about how to subvert (jail-break) its security controls is abundantly available on the Internet.
6.b(10)	Agency does not adequately monitor remote devices when connected to the agency's networks remotely in accordance with government policies (NIST 800-46, Section 3.2).	Yes	Yes, improvements are needed. The Department has several types of intrusion detection and intrusion prevention capabilities in place and is monitoring devices that establish remote connections. However, it does not have the capability to verify that the remote devices and software have a compliant security configuration, and as discussed in 6.b(2) does not require 2-factor authentication.
6.b(11)	Lost or stolen devices are not disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines)	No ⁴	We did not evaluate lost or stolen devices and the agency's or the Bureau's ability to disable the devices.
6.b(12)	Remote access rules of behavior are not adequate in accordance with government policies (NIST 800-53, PL-4).	Yes	Yes, improvements are needed. The DOI (b) (7)(E) (b) (7)(E) requires Rules of Behavior (ROB) to cover remote access. We found DOI does not have consistent Remote Access Rules of Behavior throughout all bureaus/offices.

⁴ As noted in the corresponding comment we did not evaluate lost or stolen devices and the agency's or the Bureau's ability to disable the devices. We do not have conclusive data to support this and the "No" answer reflects the inability to support a deficiency.

6.	Remote Access	Response	Comments
	Questions	Yes/No	Comments
6.b(13)	Remote access user agreements are not adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6).	Yes	Yes, improvements are needed. The DOI (b) (7)(E) (b) (7)(E) and augmenting memoranda require bureaus/offices to cover telecommuting and remote access in their Rules of Behavior. However, we found that bureau/office Rules of Behavior did not require the use of GFE, standard security configuration settings, and 2-factor authentication for all remote access. Additionally, the preconditions and requirements for permitting remote access by non-federal users are not adequately defined.

7.	Identity and Access Management	Response	Comments
	Questions	Yes/No	
7.a	The Agency has established and is maintaining an access and identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices?	No	
7.b	The Agency has established and is maintaining an identity and access management program that identifies users and network devices. However, the Agency needs to make significant improvements as noted below.	Yes	
7.b(1)	Account management policy is not fully developed.	No	No improvements needed. The DOI (b) (7)(E) (b) (7)(E) adequately meets the NIST SP-800-53, Revision 1, requirements of AC-1.
7.b(2)	Account management procedures are not fully developed and sufficiently detailed(NIST 800-53: AC-1)	Yes	Yes, improvements are needed. A Department-wide account management process has been implemented that covers all bureau/office domains; however, it is not being used by all bureaus/offices. Further, the Department has not developed and/or approved procedures that address access to DOI resources by users from entities outside DOI such as tribal organizations.
7.b(3)	Account management procedures are not consistently implemented in accordance with government policies	Yes	Yes, improvements are needed. Although Active Directory is implemented at the Department level and the Department's DOI Access system provides a standardized account management process, these tools are not across the Department for all account management functions. Implementation problems are more common with legacy and non-Windows environments. Local procedures are

7.	Identity and Access Management	Response	Comments
	Questions	Yes/No	
	(NIST 800-53: AC-2)		commonly used at bureaus/offices with large numbers of dispersed users. Further, we noted the bureaus/offices have not implemented procedures that meet government policies for users from entities outside DOI such as tribal organizations.
7.b(4)	Agency cannot identify all User and Non-User Accounts (NIST 800-53, AC-2).	Yes	Yes, improvements are needed. There is no Department-wide identity management solution in place that would assist in managing (b) (7)(E) accounts such as accounts on legacy implementations and implementations of less common operating system platforms.
7.b(5)	Accounts are not properly issued to new users (NIST 800-53, AC-2).	Yes	Yes, improvements are needed. Because there is a lack of consistency in how accounts are issued to new users, it is not feasible to ascertain at the Department level whether or not accounts are properly issued to new users.
7.b(6)	Accounts are not properly terminated when users no longer require access (NIST 800-53, AC-2).	Yes	Yes, improvements are needed. For example, we found that accounts on general support systems at 3 out of 12 bureaus/offices were not properly terminated when users no longer required access.
7.b(7)	Agency does not use multi-factor authentication where required (NIST 800-53, IA-2).	Yes	Yes, improvements are needed. In 9 of the 12 bureaus/offices reviewed there remained employees, contractors and others who require a PIV card who had not yet obtained one. Additionally, DOI has not enforced two-factor authentication for remote access for users who have the ability to use the PIV card. Some bureaus/offices reported that not all PIV cards worked as expected and forced them to leave PIV use for user authentication optional.
7.b(8)	Agency has not adequately planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11).	Yes	Yes, improvements are needed. In 9 of the 12 bureaus/offices reviewed there remained employees, contractors and others who require a PIV card who had not yet obtained one. In addition, legacy systems exist in some bureaus/offices that are not capable of using the PIV card in situations where two-factor authentication is required, such as privileged access.

7.	Identity and Access Management	Response	Comments
	Questions	Yes/No	
7.b(9)	Privileges granted are excessive or result in capability to perform conflicting functions (NIST 800-53, AC-2, and AC-6).	Yes	Yes, improvements are needed. We found the least privilege concept not being fully employed at all bureaus/offices.
7.b(10)	Agency does not use dual accounts for administrators (NIST 800-53, AC-5, and AC- 6).	No	No improvements are needed. We found that dual accounts are generally used across the Department.
7.b(11)	Network devices are not properly authenticated (NIST 800-53, IA-3).	Yes	Yes, improvements are needed. Automated techniques and tools, such as Network access control (NAC) and media access code (MAC) controls that can be used to identify devices that connect to a network, have not been consistently implemented. Even within a Bureau, some locations have such capabilities and others do not.
7.b(12)	The process for requesting or approving membership in shared privileged accounts is not adequate in accordance to government policies.	No	No improvements are needed. The DOI (b) (7)(E) prohibits the use of anonymous, guest, or shared account access unless authorized by the BCISO and requires that any use of a shared account should be documented in the application's SSP.
7.b(13)	Use of shared privileged accounts is not necessary or justified.	Yes	Yes, improvements are needed. In 6 out of 12 bureaus/offices we found the use of shared accounts that was not adequately supported and/or justified by the documented procedures.
7.b(14)	When shared accounts are used, the Agency does not renew shared account credentials when a member leaves the group.	No	No improvements are needed. We did not find instances in which this condition occurred.

8.	Continuous Monitoring	Response	
	Questions	Yes/No	Comments
8.a	The Agency has established an enterprise- wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.	No	
8.b	The Agency has established an enterprise-wide continuous monitoring program that assesses the security state of information systems. However, the Agency needs to make significant improvements as noted below.	Yes	
8.b(1)	Continuous monitoring policy is not fully developed (NIST 800-53: CA-7)	Yes	Yes, improvements are needed. As reported by the bureaus/offices, there is no comprehensive continuous monitoring policy. The Department has implemented an Internal Controls Review (ICR) process that requires that every year the bureaus/offices conduct a review of one third of the NIST 800-53 Revision 3 controls for every system. Presumably all controls would be addressed at the end of every 3-year cycle. There are also general requirements to implement real time (or near real time) automated tools for network monitoring and to conduct periodic vulnerability scans.
8.b(2)	Continuous monitoring procedures are not fully developed (NIST 800-53: CA-7)	Yes	Yes, improvements are needed. The Department produces Internal Control Review (ICR) guidance, issues Compliance Criteria, and security program data requests for its annual FISMA reviews. In part due to the variety of systems implemented throughout the DOI, procedures for network monitoring or vulnerability assessments at the Department level are not comprehensive. Most bureaus/offices implement network monitoring tools, conduct automated vulnerability testing, or both.

8.	Continuous Monitoring	Response	
	Questions	Yes/No	Comments
			Nevertheless, only some bureaus/offices have fully developed continuous monitoring procedures of their own and just point to the OCIO guidance.
8.b(3)	Continuous monitoring procedures are not consistently implemented (NIST 800-53: CA-7, 800-37 Rev1, and Appendix G).	Yes	Yes, improvements are needed. While most bureaus/offices fully participate in the Internal Control Review (ICR) process, some conducted their procedures after we had completed our review procedures. The ICR process has been in place for several years, but it does not appear to be a mature process that is uniformly implemented. The use of network monitoring tools and the use automated vulnerability testing is not done consistently across all bureaus/offices.
8.b(4)	Strategy or plan has not been fully developed for enterprise-wide continuous monitoring (NIST 800-37) Rev 1, Appendix G).	Yes	Yes, improvements are needed. As observed at the bureaus/offices, there is only a continuous monitoring strategy addressing the on-going testing of security controls, but portions addressing the use of automated vulnerability scanning and network monitoring are not fully developed. The Department conducts annual Internal Controls Review (ICR) that covers one third of the NIST 800-53 Revision 3 controls for every system every year.
8.b(5)	Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans.	Yes	Yes, improvements are needed. As observed at the bureaus/offices, most have been conducting Internal Control Reviews (ICR) testing security controls on a 3-year cycle, but some (e.g., OHA) have not been very proactive and many ICR reviews were completed after the OIG FISMA test procedures had been conducted. We also noted that OHTA did not complete an ICR given that their IT operations were in transition to OST.
8.b(6)	The following were not provided to the authorizing official or other key system officials:	Yes	
8.b(6)1	Security status reports covering continuous monitoring results	Yes	Yes, improvements are needed. Security status reporting varies by systems and is not implemented on consistent time intervals to give authorizing officials information they need to evaluate risk on an ongoing basis.
8.b(6)2	Updates to security plans	Yes	Yes, improvements are needed. Security plans were not consistently completed or updated on a quarterly basis as required by DOI policies following NIST 800-53 Revision

8.	Continuous Monitoring	Response	
	Questions	Yes/No	Comments
			3 controls. While (b) (7)(E) has been updated with Revision 3 controls and it can generate an SSP with up to date information, (b) (7)(E) is not being updated consistently by all bureaus/offices.
8.b(6)3	Security assessment reports	No	No improvements are needed. In general, the security assessment reports for the systems reviewed were included in the authorization (or accreditation) packages as appropriate at the time they were completed.
8.b(6)4	POA&Ms	Yes	Yes, improvements are needed. The POA&M process was not followed consistently as reported in the Section 5 - POA&M of this questionnaire.

9.	Contingency Planning	Response	
	Questions	Yes/No	Comments
9.a	Has the Bureau/Office established and is it maintaining an entity-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No	
9.b	The Agency has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, the Agency needs to make significant improvements as noted below.	Yes	
9.b(1)	Contingency planning policy is not fully developed, or contingency planning policy is not consistently implemented (NIST 800- 53: CP-1)	No	Yes, improvements are needed. DOI Contingency Plan policies are clearly stated in the DOI (b) (7)(E) (b) (7)(E) but it is not consistently implemented across the Department.
9.b(2)	Contingency planning procedures are not fully developed (NIST 800- 53: CP-1)	Yes	Yes, improvements are needed. While all the systems within our scope had Contingency Plans consistent with NIST 800-34 Revision 1, some bureaus/offices have not identified alternate processing sites therefore their contingency planning policy could not be considered fully developed.
9.b(3)	Contingency planning procedures are not fully developed (NIST 800- 53: CP-1)	Yes	Yes, improvements are needed. While the systems in our sample had contingency plans consistent with NIST 800-34 Revision 1, some bureaus/offices have not identified alternate processing sites and therefore their contingency plans could not be considered fully developed.

9.	Contingency Planning	Response	
	Questions	Yes/No	Comments
9.b(4)	An overall business impact assessment has not been performed (NIST SP 800-34).	No	No improvements are needed. Business Impact Assessments were generally found within the Contingency Plans of the systems within scope.
9.b(5)	Development of organization, component, or infrastructure recovery strategies and plans has not been accomplished (NIST SP 800-34).	Yes	Yes, improvements are needed. Bureau recovery strategies and plans have not been documented. System IT Contingency Plans (CP) have been completed as part of the system authorization process; however those plans do not incorporate enterprise-wide plans. The system contingency plans we reviewed do not establish a coordinated recovery strategy for Bureau information systems and operations.
9.b(6)	A business continuity/disaster recovery plan has not been developed (FCD1, NIST SP 800-34).	Yes	Yes, improvements are needed. DOI guidance details the requirements associated with the system Contingency Plan as part of the authorization process. Bureaus/Offices do not have documented Business Continuity or Disaster Recovery Plans.
9.b(7)	A business continuity/disaster recovery plan has been developed, but not fully implemented (FCD1, NIST SP 800-34).	Yes	Yes, improvements are needed. While the systems in our sample had contingency plans consistent with NIST 800-34 Revision 1, business continuity/disaster recovery plans have not been documented. In addition, two bureaus/offices have open POA&Ms for the lack of alternate processing sites.
9.b(8)	System contingency plans missing or incomplete (FCD1, NIST SP 800-34, NIST SP 800-53).	Yes	Yes, improvements are needed. While the systems in our sample had contingency plans consistent with NIST 800-34 Revision 1, some bureaus/offices have not identified alternate processing sites and therefore their contingency plans could not be considered fully developed. Two bureaus/offices have open POA&Ms for the lack of alternate processing sites.
9.b(9)	Systems contingency plans are not tested (FCD1, NIST SP 800- 34, NIST SP 800-53).	Yes	Yes, improvements are needed. There was no evidence of contingency plan testing in the last year for systems at 3 out of 12 bureaus.
9.b(10)	Test, training, and exercise programs have not been developed (FCD1, NIST SP 800-	Yes	Yes, improvements are needed. Training, testing and exercises have not been fully developed at the Departmental level and consistently implemented at the bureau/office level.

9.	Contingency Planning	Response	
	Questions	Yes/No	Comments
	34, and NIST 800-53).		
9.b(11)	Test, training, and exercise programs have been developed, but are not fully implemented (FCD1, NIST SP 800-34, NIST SP 800-53).	Yes	Yes, improvements are needed. Training, testing and exercises have not been fully developed and thus not implemented. For example, business continuity testing is not documented and therefore not conducted at NBC.
9.b(12)	After-action report did not address issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800- 34).	Yes	Yes, improvements are needed. Contingency/disaster recovery exercises were not conducted consistently this year and therefore after action reports were not available.
9.b(13)	Systems do not have alternate processing sites (FCD1, NIST SP 800-34, and NIST SP 800-53).	Yes	Yes, improvements are needed. Not all bureaus/offices have identified alternate processing sites for all critical operations. Two bureaus had open POA&Ms for not identifying alternate processing sites for use in case of disruption to their operations.
9.b(14)	Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, and NIST SP 800-53).	No ⁵	We did not determine the distance between primary processing sites and alternate processing sites for all systems or environmental similarities that could result in the same risks at both sites.
9.b(15)	Backups of information are not performed in a timely manner (FCD1, NIST SP 800-34, and NIST SP 800-53).	No	No improvements are needed. Regular backups were scheduled for the systems tested.
9.b(16)	Backups are not appropriately tested (FCD1, NIST SP 800- 34, NIST SP 800-53).	No	No improvements are needed. While we found an instance at one bureau where data loss occurred because backups were not tested, it appears backups are generally tested across the Department.

-

⁵ As stated in the corresponding comment, we did not determine the distance between primary processing sites and alternate processing sites for all systems or environmental similarities that could result in the same risks at both sites. We do not have conclusive data to support this and the "No" answer reflects the inability to support a deficiency.

9.	Contingency Planning	Response	Comments
	Questions	Yes/No	Comments
9.b(17)	Backups are not properly secured and protected (FCD1, NIST SP 800-34, and NIST SP 800-53).	No	No improvements are needed. All the systems we tested had contracts in place for the off-site storage of backups.
9.b(18)	Contingency planning does not consider supply chain threats.	Yes	Yes, improvements are needed. None of the DOI contingency planning guidance we reviewed addressed supply chain threats.

10.	Contractor Systems	Response	
	Questions	Yes/No	Comments
10.a	The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency.	No	
10.b	The Agency has established and maintains a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in public cloud. However, the Agency needs to make significant improvements as noted below.	Yes	
10.b(1)	Policies to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not fully developed.	Yes	Yes, improvements are needed. The DOI (b) (7)(E) (b) (7)(E) does not adequately define contractor systems and contractor oversight responsibilities. The (b) (7)(E) provides limited details regarding requirements for performing contractor oversight. No DOI systems are currently residing in a public cloud and there are no DOI policies specifically addressing services residing in a public cloud.
10.b(2)	Procedures to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud, are not	Yes	Yes improvements are needed. The DOI (b) (7)(E) does not provide sufficiently developed procedures for performing contractor oversight. 6 of the 12 bureaus/offices have contractor systems in the (b) (7)(E) system inventory for a combined total of 18 contractor systems. Of the 6 bureaus/offices that have contractor systems, only one has augmented the DOI

10.	Contractor Systems	Response	
	Questions	Yes/No	Comments
	fully developed.		policies with their own policies.
10.b(3)	Procedures to oversee systems operated on the Agency's behalf by contractors or other entities, including Agency systems and services residing in public cloud are not consistently implemented.	Yes	Yes, improvements are needed. One of the contractor systems in our sample was decommissioned, but the other two did not follow oversight procedures consistently. No DOI systems are currently residing in a public cloud.
10.b(4)	The inventory of systems owned or operated by contractors or other entities, including Agency systems and services residing in public cloud, is not complete in accordance with government policies (NIST 800-53: PM-5).	Yes	Yes, improvements are needed. Because there is no Departmental definition of contractor system that is consistent with OMB requirements, it is not possible to assess the completeness of the inventory. There are external service providers that conduct IT security operations for DOI and at least some of its bureaus/offices that could have been included in such an inventory depending on the definition applied.
10.b(5)	The inventory does not identify interfaces between contractor/entity-operated systems to Agency owned and operated systems.	Yes	Yes, improvements are needed. Although (1) (7)(E) provides the capability to record system interfaces, interfaces were only shown for a third of the contractor system. We found that contractor interfaces were usually described in pre- (1) (7)(E) system security plans, but the Department's shift to using (1) (7)(E) to create System Security Plans means those are being phased out.
10.b(6)	The inventory of contractor/entity-operated systems, including interfaces, is not updated at least annually.	Yes	Yes, improvements are needed. Bureaus/Offices are not consistently updating their inventory of contractor systems and the interfaces of those systems with entity-operated systems.
10.b(7)	Systems owned or operated by contractors and entities are not subject to NIST and OMB's FISMA requirements (e.g., security requirements).	No	No improvements are needed. All three contractor systems within the scope of our review had gone through Certification and Accreditation in accordance with NIST SP 800-53 Revision 1. The continued compliance of these systems with NIST requirements is monitored by including them in the annual ICR.

10.	Contractor Systems	Response	Comments
	Questions	Yes/No	Comments
10.b(8)	Systems owned or operated by contractor's and entities do not meet NIST and OMB's FISMA requirements (e.g., security requirements).	No	No improvements are needed. All three contractor systems within the scope of our review had gone through Certification and Accreditation in accordance with NIST SP 800-53. An annual internal controls review had also been performed for each of the systems.
10.b(9)	Interface agreements (e.g., MOUs) are not properly documented, authorized, or maintained.	Yes	Yes, improvements are needed. Contractor system interfaces are not consistently documented, and none of the 3 contractor systems within the scope of our review had information in about the concerning interface or interconnection security agreements. At least one of these systems exchanges information with a system outside of DOI based on a Memorandum of Agreement.

11.	Security Capital Planning	Response	
	Questions	Yes/No	Comments
11.a	The Agency has established and is maintaining a security architecture and capital planning investment program for information security?	No	
11.a(1)	Documented policies and procedures to address information security in the capital planning and investment control process.	Yes	No improvement needed. The Department issues annual guidance, as well as formulation/submission related guidance, that require security costs to be reported on OMB Exhibit 53 form in accordance with OMB A-11 section 53 A and B requirements. Procedural guidance instructs bureaus/offices to separately enter security costs on Exhibit 53A, Exhibit 300A, Exhibit 300B Section C under the category "Infrastructure Contributions," updating the contracts table on the line" <bureau> - BY13 Infrastructure - Security Management - Input Form." In addition Exhibit 53B captures security data at the portfolio/not the investment level.</bureau>
11.a.(2)	Includes information security requirements as part of the capital planning and investment process.	Yes	No improvement needed. The Department issues annual guidance, as well as formulation/submission related guidance, that require security costs to be reported on OMB Exhibit 53 form in accordance with OMB A-11 section 53 A and B requirements.
11.a.(3)	Establishes a discrete line item for information security in organizational programming and documentation.	Yes	No improvement needed. The bureaus/offices follow procedural guidance that instructs them to separately enter security costs on Exhibit 53A, Exhibit 300A, Exhibit 300B Section C under the category "Infrastructure Contributions," updating the contracts table on the line" <bureau> - BY13 Infrastructure - Security Management - Input Form." In addition Exhibit 53B captures security data at the portfolio/not the investment level.</bureau>
11.a.(4)	Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required.	Yes	No improvement needed. Procedural guidance instructs bureaus/offices to separately enter security costs on Exhibit 53A, Exhibit 300A, Exhibit 300B Section C under the category "Infrastructure Contributions," updating the contracts table on the line" <bureau> - BY13 Infrastructure - Security Management - Input Form." In addition Exhibit 53B captures security data at the portfolio/not the investment level.</bureau>
11.a(5)	Ensures that information security resources are available for expenditure as planned	Yes ⁶	The Agency adequately plans for IT security during the (b) (7)(E), but the scope of our work does not allow us to test the adequacy or availability of the funds planned for by DOI.

_

⁶ As noted in the corresponding comment, the testing of this control goes beyond the time window for the scope of our procedures and does not allow us to test the adequacy or availability of the funds planned for by DOI. We do not have conclusive data to support this and the "Yes" answer reflects the inability to support a deficiency.



INDEPENDENT AUDITORS' PERFORMANCE
AUDIT REPORT ON THE U.S. DEPARTMENT
OF THE INTERIOR FEDERAL INFORMATION
SECURITY MANAGEMENT ACT FOR
FISCAL YEAR 2015

Report No.: 2015-ITA-072 February 2016



Memorandum

FEB 2 4 2016

To:

Sylvia Burns

Chief Information Officer

From:

Mary L. Kendall

Deputy Inspector General

Subject:

Independent Auditors' Performance Audit Report on the U.S. Department of the

Interior Federal Information Security Management Act for Fiscal Year 2015

Report No. 2015-ITA-072

This memorandum transmits the KPMG LLP (KPMG) Federal Information Security Management Act (FISMA) audit report of the U.S. Department of the Interior (DOI) for fiscal year (FY) 2015. FISMA (Public Law 107-347) requires Federal agencies to have an annual independent evaluation of their information security programs and practices performed by their Office of Inspector General (OIG) or by an independent external auditor, as determined by their OIG, to determine the effectiveness of such programs and practices.

KPMG, an independent public accounting firm, performed the DOI FY 2015 FISMA audit under a contract issued by DOI and monitored by OIG. As required by the contract, KPMG asserted that it conducted the audit in accordance with Generally Accepted Government Auditing Standards to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. KPMG is responsible for the findings and conclusions expressed in the audit report. OIG does not express an opinion on the report, nor on KPMG's conclusions regarding DOI's compliance with laws and regulations.

FISMA reporting has been completed in accordance with Office of Management and Budget Memorandum M-16-03, "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements," dated October 30, 2015.

KPMG reviewed information security practices, policies, and procedures at the DOI Office of the Chief Information Officer and 12 DOI bureaus and offices:

- Bureau of Indian Affairs;
- Bureau of Land Management;
- Bureau of Reclamation;
- Bureau of Safety and Environmental Enforcement;
- U.S. Fish and Wildlife Service;
- National Park Service:
- Office of Inspector General;

- Office of The Secretary;
- Office of Surface Mining Reclamation and Enforcement;
- Office of the Solicitor;
- Office of the Special Trustee for American Indians; and the
- U.S. Geological Survey.

To ensure the quality of the audit work, we—

- reviewed KPMG's approach and planning of the audit;
- evaluated the auditors' qualifications and independence;
- monitored the audit's progress at key milestones;
- engaged in regularly scheduled meetings with KPMG and DOI management to discuss audit progress, findings, and recommendations;
- reviewed KPMG's supporting work papers and audit report; and
- performed other procedures as deemed necessary.

KPMG identified needed improvements in most areas audited including continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestone, remote access management, and contingency planning. KPMG made 59 recommendations intended to strengthen DOI's information security program. In its response to the draft report, the Office of the Chief Information Officer concurred with all recommendations, and stated it was in the process of taking or would take corrective actions.

We will refer KPMG's recommendations to the Office of Financial Management for audit follow-up. The legislation creating OIG requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement recommendations; and recommendations that have not been implemented.

We appreciate the cooperation and assistance of DOI personnel during the audit. If you have any questions regarding the report, please contact me at 202–208–5745.

Attachment

The United States Department of the Interior Office of Inspector General Federal Information Security Management Act Fiscal Year 2015 Performance Audit



February 4, 2016



February 4, 2016

Ms. Mary L. Kendall Deputy Inspector General U.S. Department of the Interior Office of Inspector General 1849 C Street, NW MS 4428 Washington, DC 20240-0001

Dear Ms. Kendall:

This report presents the results of our work conducted to address the performance audit objectives relative to the Fiscal Year (FY) 2015 Federal Information Security Management Act (FISMA) Audit for information systems. We performed our work during the period of April 23 to September 30, 2015 and our results are as of February 4, 2016.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The audit objective(s) of our work were to for the year ending September 30, 2015:

- Perform the annual independent FISMA audit of DOI's information security programs and practices related to the financial and non-financial information systems in accordance with the FISMA, Public Law 107-347.
- Assess the implementation of the security control catalog contained in the National Institute of
 Standards and Technology (NIST) Special Publication (SP) 800-53 Revision (Rev) 3. We utilized
 criteria and guidance, including Federal Information Processing Standard (FIPS) Publication (PUB)
 199, FIPS PUB 200, NIST SP 800-37 Rev 1, and NIST SP 800-53 Rev 3. Criteria and guidance were
 used to evaluate DOI's implementation of the risk management framework and the extent of
 implementation of select security controls.
- Prepare responses for each of the Department of Homeland Security (DHS) FISMA Reporting Metrics on behalf of the DOI Office of Inspector General (OIG) to support documented conclusions with appropriate rationale/justification as to the effectiveness of the information security program and practices of the DOI for each area evaluated and overall.

Our procedures tested security control areas identified in NIST SP 800-53 and additional security program areas identified in the 2015 FISMA Reporting Metrics for the OIG. Our sample was selected from information systems distributed across 13 Bureaus/Offices. These Bureaus/Offices are Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE), National Park Service (NPS), Office of the Chief Information Officer (OCIO), Office of Inspector General (OIG), Office of the Secretary (OS), Office of Surface Mining Reclamation and Enforcement (OSMRE), the Office of the Special Trustee for American Indians (OST), Office of the Solicitor (SOL), U.S. Fish and Wildlife Service (FWS), and U.S. Geological Survey (USGS). At the conclusion of our test procedures, we aggregated the individual bureau and information system results by control area to produce results at the Department level.

As part of the FISMA performance audit of the subset of DOI information systems, we assessed the effectiveness of the Department's information security program and practices and the implementation of the security controls in NIST SP 800-53 Revision 3. We identified needed improvements in most areas audited including continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestone, remote access management, and contingency planning.

The following table summarizes the control areas tested and the weaknesses identified in the 2015 FISMA Reporting Metrics for the OIG.

2015 FISMA Program Area	Findings/Results Summary				
1. Continuous Monitoring Management	DOI has established a continuous monitoring management program. However, opportunities for improvement exist:				
	Ensure stakeholders have adequate resources to effectively implement continuous monitoring management activities;				
	Identify and define qualitative and quantitative performance measures to assess the effectiveness of the program;				
	Define processes for collecting and considering lessons learned to improve continuous monitoring processes;				
	Identify and define technologies needed to fully implement the program, such as license management, information management, software assurance, event management, network management, malware detection, and incident management; and				
	Define automation to produce an accurate point-in-time inventory of authorized and unauthorized devices and software on the DOI network.				
Configuration Management	DOI has established a configuration management program. However, DOI has not fully:				
	developed and documented baseline security configurations for Linux servers;				
	assessed compliance with documented baseline configurations;				
	 disabled vulnerable ports and services, such as (b) (7)(E); and implemented (b) (7)(E) in accordance with DOI policy. 				
3. Identity & Access Management	DOI has established an identity and access management program to identify users and network devices. However, DOI has not fully:				
	 documented an account management (b) (7)(E) (b) (7)(E) 				
	 performed and documented (b) (7)(E) 				
	• implemented a process to (b) (7)(E) and				

2015 FISMA Program Area	Findings/Results Summary
	 managed user accounts to ensure user accounts are (b) (7)(E) (b) (7)(E)
4. Incident Response and Reporting	DOI has establish an incident response and reporting program. However, DOI has not fully:
	updated relevant incident response and reporting policies and procedures; and
	 maintained evidence of information system (b) (7)(E) (b) (7)(E)
5. Risk Management	DOI has established and is maintaining a risk management program. However, DOI has not fully:
	updated information within the system security plan, to include system security plans to ensure information is complete and accurate; and
	 completed the risk management framework activities to include authorizing (b) (7)(E)
6. Security Training	DOI has established and is maintaining a security training program. However, DOI has not fully:
	conducted specialized training, such as Role Based Security Training for all personnel with significant information security responsibilities.
7. Plan of Action and Milestones	DOI has established and is maintaining a plan of action and milestone program. However, DOI has not fully:
	conducted quarterly reviews over two program-level plan of action and milestones.
8. Remote Access Management	DOI has established and is maintaining a remote access management program. However, DOI has not fully:
	remediated prior year remote access management recommendations;
	• required (b) (7)(E) for all remote access solutions.
9. Contingency Planning	DOI has established and is maintaining an enterprise-wide business continuity/disaster recovery program. However, DOI has not fully:
	 ensured mission essential functions are documented in continuity of operations plans;
	tested continuity of operations and information system contingency plans annually; and
	• ensured (b) (7)(E) are performed in accordance with DOI policy.

We have made 59 recommendations related to these weaknesses intended to strengthen the respective Bureaus, Offices, and the Department's information security program. Also, the report includes six appendices, Appendix I summarizes the program areas in which bureaus have control deficiencies, Appendix II list of acronyms, Appendix III provides the status of prior year recommendations; 38 of 56 (68%) remain open, Appendix IV lists the NIST Special Publication 800-53 security controls cross-referenced to the FY2015 OIG FISMA metrics, Appendix V provides the FY2015 OIG FISMA Reporting metrics, and Appendix VI provides the description of the information security continuous monitoring maturity model for FY2015.

This performance audit did not constitute an audit of financial statements in accordance with *Government Auditing Standards*. KPMG was not engaged to, and did not; render an opinion on the U.S. Department of the Interior's internal controls over financial reporting or over financial management systems. KPMG cautions that projecting the results of our evaluation to future periods is subject to the risks that controls may become inadequate because of changes in conditions or because compliance with controls may deteriorate.



The United States Department of the Interior Office of Inspector General Federal Information Security Management Act - Fiscal Year 2015 Performance Audit

Table of Contents

٦	

Background	7
Mission of the DOI and its Bureaus/Offices	
Information Technology (IT) Organization	8
FISMA	8
Objective, Scope, and Methodology	
Results of Review	
1. Continuous Monitoring Management Program Opportunities for Improvement	13
2. Implementation of the Configuration Management Program Needs Improvement	14
3. Implementation of the Identity and Access Management Program Needs Improvement	22
4. Implementation of the Incident Response and Reporting Program Needs Improvement	26
5. Implementation of the Risk Management Program Needs Improvement	30
6. Implementation of the Security Training Program Needs Improvement	32
7. Implementation of the Plan of Action and Milestones Program Needs Improvement	34
8. Implementation of the Contingency Planning Program Needs Improvement	35
Conclusion	. 38
Management Response to Report	. 39
Appendix I – Summary of FISMA Program Areas	.48
Appendix II – Listing of Acronyms	. 54
Appendix III – Prior Year Recommendation Status	. 59
Appendix IV - NIST SP 800-53 Security Controls Cross-Referenced to FY2015 OIG FISMA Metrics	. 72
Appendix V – 2015 FISMA Reporting Metrics	. 74
Appendix VI – Information Security Continuous Monitoring Maturity Model for Fiscal Year 2015.	
Source : Council of the Inspector General for Integrity and Efficiency (CIGIE)	. 79

Background

Mission of the DOI and its Bureaus/Offices

The U.S. Department of the Interior (DOI) protects America's natural resources and heritage, honors our cultures and tribal communities, and supplies the energy to power our future. DOI is composed of a number of Bureaus and a number of additional Offices that fall under the Office of the Secretary, the Assistant Secretary for Policy, Management and Budget, Solicitor's Office and Office of Inspector General. Of those, the following 13¹ Bureaus and Offices are included within the scope of the Office of Inspector General's (OIG) FISMA reporting for 2015:

- 1 The <u>Bureau of Indian Affairs (BIA)</u> is responsible for the administration and management of 55 million surface acres and 57 million acres of subsurface minerals estates held in trust by the United States for American Indian, Indian tribes, and Alaska Natives.
- 2 The <u>Bureau of Land Management (BLM)</u> administers 262 million surface acres of America's public lands, located primarily in 12 Western States. The BLM sustains the health, diversity, and productivity of the public lands for the use and enjoyment of present and future generations.
- The <u>Bureau of Reclamation (BOR)</u> manages, develops, and protects water and related resources in an environmentally and economically sound manner in the interest of the American public.
- 4 The <u>Bureau of Safety and Environmental Enforcement (BSEE)</u> is responsible for overseeing the safe and environmentally responsible development of energy and mineral resources on the Outer Continental Shelf.
- 5 The <u>U.S. Fish and Wildlife Service (FWS)</u> was created to conserve, protect, and enhance fish, wildlife, and plants and their habitats for the continuing benefit of the American people.
- 6 The <u>National Park Service (NPS)</u> supports to preserve unimpaired the natural and cultural resources and values of the national park system, a network of nearly 400 natural, cultural, and recreational sites across the nation, for the enjoyment, education, and inspiration of this and future generations.
- 7 The Office of the Chief Information Officer (OCIO) provides the executive leadership, policy, guidance, independent program evaluation, and coordination needed to manage the diverse, complex, nationally significant programs that are DOI's responsibility. These Offices also guide and coordinate all of DOI's administrative activities such as finance, information resources, procurement and acquisition, human resources, and budgeting.
- 8 The <u>Office of the Inspector General (OIG)</u> accomplishes its mission by performing audits, investigations, evaluations, inspections, and other reviews of the DOI's programs and operations. They independently and objectively identify risks and vulnerabilities that directly affect, or could impact, DOI's mission and the vast responsibilities of its bureaus and entities. Their objective is to improve the accountability of DOI and their responsiveness to Congress, the Department, and the public.
- 9 The <u>Office of the Secretary (OS)</u> is primarily responsible for providing quality services and efficient solutions to meet DOI business needs through its most important asset its people.

¹. Our sample resulted in a subset of information systems distributed over 13 Bureaus/Offices.

- 10 The Office of Surface Mining (OSMRE) carries out the requirements of the Surface Mining Control and Reclamation Act in cooperation with States and Tribes. Their primary objectives are to ensure that coal mines are operated in a manner that protects citizens and the environment during mining and assures the land is restored to beneficial use following mining, and to mitigate the effects of past mining by aggressively pursuing reclamation of abandoned coal mines.
- 11 The <u>Office of the Special Trustee for American Indians (OST)</u> improves the accountability and management of Indian funds held in trust by the federal government.
- 12 The <u>Office of the Solicitor (SOL)</u> performs the legal work for the United States Department of the Interior, manages the Department's Ethics Office and resolves FOIA Appeals.
- 13 The <u>U.S. Geological Survey (USGS)</u> serves the nation by providing reliable scientific information to describe and understand the earth; minimize loss of life and property from natural disasters; manage water, biological, energy, and mineral resources; and enhance and protect our quality of life.

Information Technology (IT) Organization

The Office of the Chief Information Officer (OCIO) heads the security management program for the Department. The Chief Information Security Officer (CISO) serves as the head of the OCIO's Information Management and Assurance Division, assumed responsibility of all Information Assurance (IA) functions within the OCIO as CISO. The Bureaus/Offices have an Associate Director for Information Resources (ADIR) whose role is roughly equivalent to that of a Bureau Chief Information Officer. Many Bureaus/Offices also have Bureau Chief Information Security Officers (BCISOs) that are responsible for the local implementation of the Department's information security program.

FISMA

Federal Information Security Modernization Act of 2014 - Amends the Federal Information Security Management Act of 2002 (FISMA) to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices, and (2) set forth authority for the Secretary of Homeland Security (DHS) to administer the implementation of such policies and practices for information systems. Additional enhancements to the federal law:

- Reasserts the authority of the Director of the Office of Management and Budget (OMB) with
 oversight, while authorizing the Secretary of the Department of Homeland Security (DHS) to
 administer the implementation of security policies and practices for Federal Information Systems.
 Gives the delegation of OMB's authorities to the Director of National Intelligence (DNI) for systems
 operated by an element of the intelligence community.
- Requires agencies to notify Congress of major security incidents within seven days. OMB is responsible for developing guidance on what constitutes a major incident.
- Places more responsibility on agencies looking at budgetary planning for security management, ensuring senior officials accomplish information security tasks, and that all personnel are responsible for complying with agency information security programs.
- Changes the reporting guidance focusing on threats, vulnerabilities, incidents, the compliance status of systems at the time of major incidents, and data on incidents involving personally identifiable information (PII).

 Provides for the use of automated tools in agencies' information security programs, including periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents.

Objective, Scope, and Methodology

The objectives for this performance audit were to for the year ending September 30, 2015:

- Perform the annual independent Federal Information Systems Security Management (FISMA) audit of DOI's information security programs and practices related to the financial and non-financial information systems in accordance with the FISMA, Public Law 107-347.
- Assess the implementation of the security control catalog contained in the NIST SP 800-53 Rev 3. We utilized criteria and guidance, including FIPS 199, FIPS 200, and NIST SP 800-53 Rev 3, to evaluate the implementation of the risk management framework and the extent of implementation of security controls selected from the security control catalog. The table in Appendix IV lists the NIST SP 800-53 revision 3 controls² considered during the performance audit.
- Prepare responses for each of the OMB/Department of Homeland Security (DHS) FISMA Reporting Metrics on behalf of the DOI OIG to support documented conclusions on the effectiveness of the information security program and practices of the DOI for each area evaluated.

The scope of our audit included the following:

- An inspection of relevant information security practices and policies established by the DOI Office of the Chief Information Officer (OCIO) as they relate to the FY2015 OIG FISMA reporting metrics; and
- An inspection of the information security practices, policies, and procedures in use across 13 Bureaus and Offices identified by the DOI OIG, specifically, BIA, BLM, BOR, BSEE, FWS, NPS, OCIO, OIG, OS, OSMRE, OST, SOL, and USGS.

Specifically, our approach followed two steps:

Step A: Department and Bureau level Compliance – During this step we gained Department and Bureau understanding of the FISMA-related policies and guidance established by the DOI OCIO. We compared the policies, procedures, and practices established to the applicable Federal laws and criteria to evaluate whether the Department and Bureaus are generally consistent with FISMA.

Step B: Assessment of the implementation of select security controls from the NIST SP 800-53 revision 3. During this process, we assessed the implementation of a selection of security controls from the NIST SP 800-53 Rev 3, for our representative subset (10 %) of DOI's information systems.³

_

² The Department is in the process of updating relevant information security policies and procedures in accordance with NIST SP 800-53 revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, with an anticipated completion date of December 31, 2015.

³ In accordance with the Request for Quotation (RFQ) No. D11PS40153 for Financial Audit Services for the U.S. Department of the Interior, Office of the Inspector General RFQ# D 11PD40 153 Financial Audit Services, dated January 26, 2011; we employed a random sampling approach to determine a representative subset of 10 percent of the DOI information systems. That representative subset includes Major Applications and General Support Systems with Federal Information Processing Standard (FIPS) 199 security categorizations of "Low," "Moderate," and "High". The FIPS 199 ratings are defined by the DOI system owner and authorizing official. We randomly selected 13 systems, which represents 10 percent of the total DOI information systems recorded in CSAM.

The controls selected addressed areas covered by the DHS FY2015 Inspector General Federal Information Security Management Act Reporting Metrics.

The DOI Statement of Work (SOW) for the FISMA audit required us to perform our procedures on a subset of systems defined by the Department as at least 10% of the information systems in the DOI's authoritative information system inventory in the Cyber Security Assessment and Management (CSAM) application. The table below identifies the information systems audited.

Table 1. DOI Information Systems Audited

BUREAU OF INDIAN AFFAIRS							
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location		
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)		

BUREAU OF LAND MANAGEMENT							
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location		
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)		

BUREAU OF RECLAMATION							
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location		
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)		

BUREAU OF SAFETY AND ENVIRONMENTAL ENFORCEMENT							
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location		
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)		

U.S. FISH AND WILDLIFE SERVICE							
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location		
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)		

OFFICE OF THE CHIEF INFORMATION OFFICER						
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location	
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)	

NATIONAL PARKS SERVICE						
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location	
(b) (5)	(b) (5)	(b) (5)	Moderate	(b) (5)	(b) (5)	

OFFICE OF THE INSPECTOR GENERAL					
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)

OFFICE OF THE SECRETARY					
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)

OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT					
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location
(b) (7)(E)	(b) (7)(E)	(O) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)

OFFICE OF THE SOLICITOR					
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)

OFFICE OF THE SPECIAL TRUSTEE FOR AMERICAN INDIANS					
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Moderate	(b) (7)(E)	(b) (7)(E)

U.S. GEOLOGICAL SURVEY					
System Name	Acronym	CSAM ID	FIPS 199 Category	Туре	Location
(b) (7)(E)	(b) (7)(E)	(b) (7)(E)	Low	(b) (7)(E)	(b) (7)(E)

Results of Review

We identified needed improvements in most audited including continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestone, remote access management, and contingency planning.

1. Continuous Monitoring Management Program Opportunities for Improvement

KPMG inquired of personnel responsible for establishing, implementing, and maintaining the DOI continuous monitoring management program, reviewed applicable documentation, and determined that the maturity level for the People domain is level two, Defined, Processes and Technology domains level one, Ad-hoc. The overall DOI continuous monitoring management program maturity level rated level one, Ad-hoc. In accordance with the Office of Management and Budget, Memorandum M-14-03, Subject: *Enhancing the Security of Federal Information and Information Systems*, dated November 18, 2013 the Information Security Continuous Monitoring program is expected to be fully implemented by December 2017.

The purpose of the maturity model is to (1) summarize the status of DOI's information security programs and its maturity on a 5-level scale, (2) provide transparency to agency CIOs, top management officials, and other interested readers of OIG FISMA report about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level, and (3) help ensure consistency across the Federal Government OIGs in their annual FISMA audits. Appendix VI below defines each maturity level.

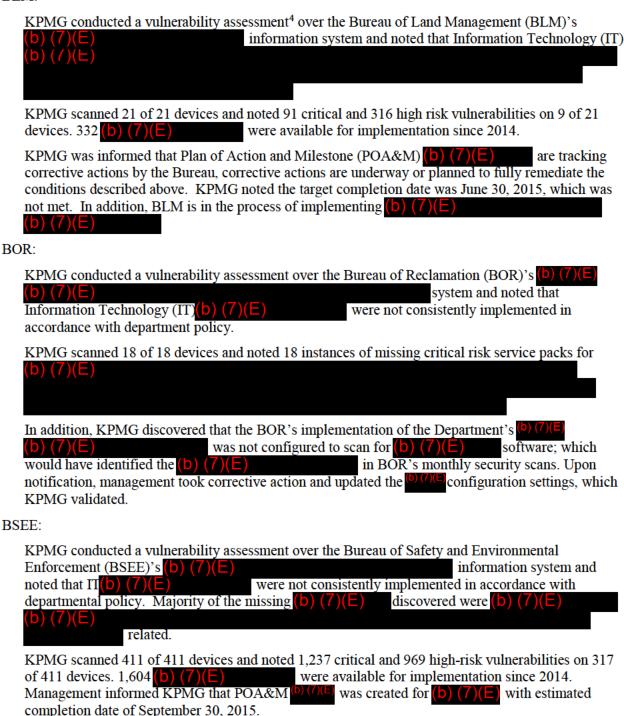
KPMG noted the following opportunities for improvement:

- People Domain: The Department has defined responsibilities for Information Security Continuous Monitoring (ISCM) stakeholders; however, stakeholders may not have adequate resources (people, processes, and technology) to implement ISCM activities.
- Processes Domain: The Department has not identified and defined the qualitative and quantitative
 performance measures that will be used to assess the effectiveness of its ISCM program, achieve
 situational awareness, and control ongoing risk. In addition, the Department has not defined its
 processes for collecting and considering lessons learned to improve ISCM processes.
- Technology Domain: The Department has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. The Department ISCM program focuses on four security automation controls areas such as vulnerability management, patch management, asset management and configuration management; however, the use of ISCM technologies in the following areas are not fully defined, license management, information management, software assurance, event management, network management, malware detection and incident management. In addition, the Department has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network.

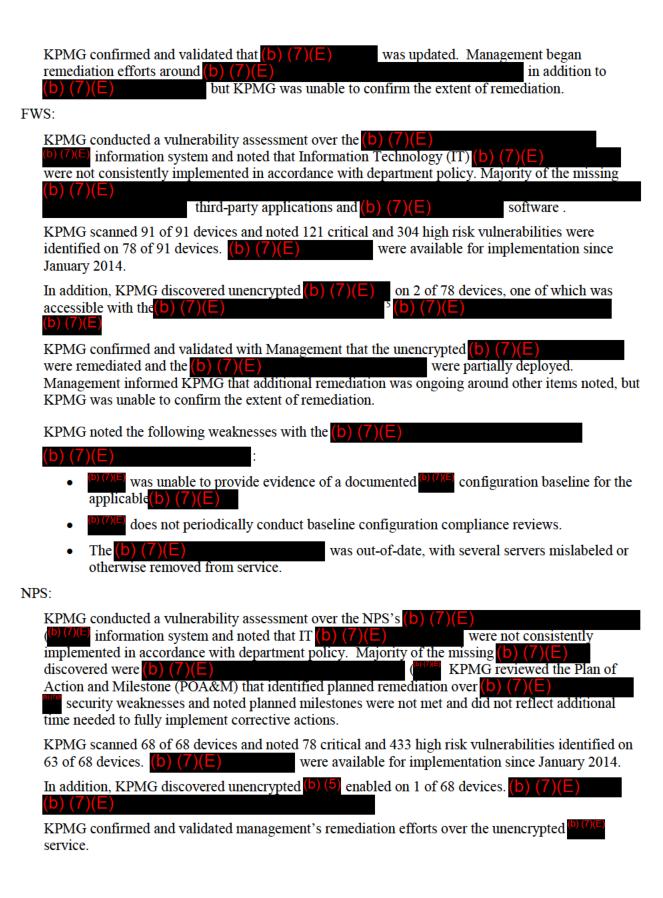
2. Implementation of the Configuration Management Program Needs Improvement

KPMG noted the following weaknesses at 10 of 13 bureaus and offices, BLM, BOR, BSEE, FWS, NPS, OCIO, OSMRE, OST, USGS, and SOL configuration management programs:

BLM:



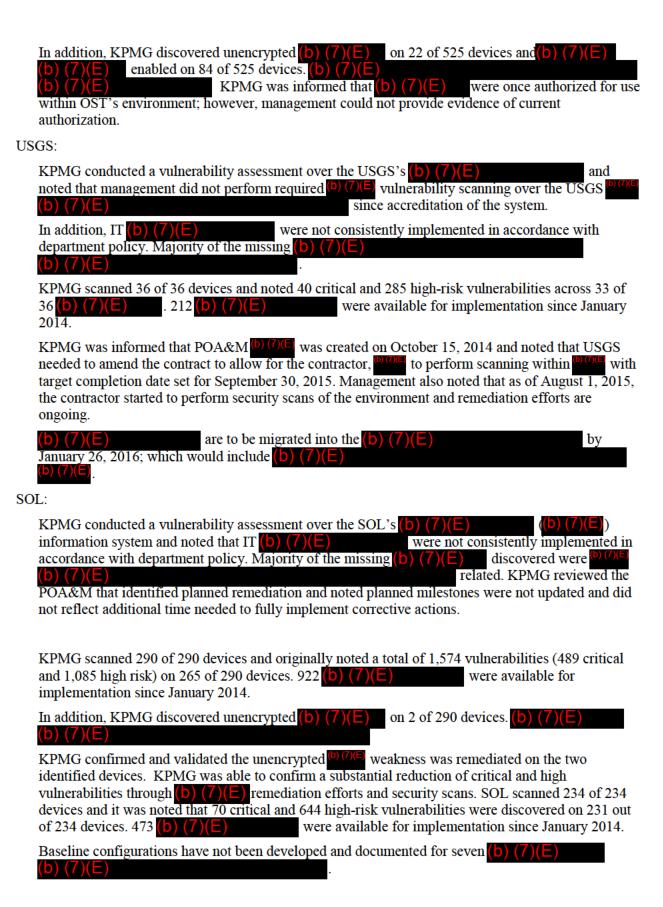
⁴ Vulnerability assessment is a process to identify security flaws and weaknesses in a computer, network, or application.



⁵(b) (7)(E)

OCIO:

KPMG conducted a vulnerability assessment over the Office of the Secretary (OS)'s information system b) (7)(E) by **(b** and noted that IT (b) (7)(E) were not consistently implemented in accordance with department policy. Majority of the missing (b) (7)(E) discovered were (b) (7)(E)related. KPMG scanned 330 of 330 devices and noted 1,496 high-risk vulnerabilities on 111 devices. Two had 761 missing (b) (7)(E). Vulnerabilities identified could allow unauthorized access to the (b) (7)(E) and provide unauthorized access to (b) (7)(E) In addition, KPMG noted that (b) (7)(E) vulnerability scanning over the (b) (7)(E) was not being performed with proper authentication. Authenticated scans provide more accurate vulnerability information by authenticating to scanned devices to obtain detailed and accurate information about the operating system and installed software, including configuration issues and missing security patches. Upon notification, the Office of Chief Information Officer (OCIO) Security personnel corrected the scanning configuration and KPMG validated the configuration setting. KPMG discovered unencrypted (b) (7)(E)(b) (7)(E) enabled on 2 of 330 network devices. (b) (7)(E)KPMG confirmed and validated management's remediation efforts and noted a significant reduction of vulnerabilities. The original 761 high-risk items were reduced to 206 high-risk items. Management also informed KPMG that additional remediation was ongoing, but KPMG was unable to confirm the extent of the remediation. OSMRE: KPMG conducted a vulnerability assessment over OSMRE's (b) (7)(E)) and noted that IT (b) (7)(E)were not consistently implemented in accordance with department policy. Majority of the missing (b) (7)(E) discovered were (b) (7)(E)related. KPMG scanned 162 of 162 devices and noted 255 critical and 1,408 high risk vulnerabilities were identified on 162 devices. 901 (b) (7)(E) were available for implementation since January 2014. In addition, KPMG discovered unencrypted (b) (7)(E) on 4 of 162 devices. Management informed KPMG that 3 of 4 (b) (7)(E) were disabled, and additional remediation ongoing; however, KPMG was unable to validate the extent of the remediation. OST: KPMG conducted a vulnerability assessment over the OST's (b) (7)(=) and noted that IT(b) (7)(E) were not consistently implemented in accordance with department policy. Majority of the missing (b) (7)(E) discovered were (b) (7)(E)KPMG considered OST's (b) (7)(E) strategy and noted the vulnerabilities that extended beyond the (b) (7)(E) for critical and high-risk vulnerabilities. KPMG scanned 525 of 525 devices and noted 2,225 critical and 3,952 high-risk vulnerabilities on 416 of 525 devices. 4,597 were available for implementation since January 2014.



Department of the Interior, Security Control Standard, Risk Assessment version 1.3, dated December 2012, RA-5 Vulnerability Scanning states:

"Control: The organization:

- a. Scans for vulnerabilities in the information system and hosted applications quarterly for operating system(s), web application(s), and database(s) (as applicable) and when new vulnerabilities potentially affecting the system/applications are identified and reported;
- b. Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - Enumerating platforms, software flaws, and improper configurations;
 - Formatting and making transparent, checklists and test procedures; and
 - Measuring vulnerability impact;
- c. Analyzes vulnerability scan reports and results from security control assessments;
- d. Remediates legitimate vulnerabilities within thirty days for high-risk vulnerabilities; within ninety days for moderate risk vulnerabilities in accordance with an organizational assessment of risk; and
- e. Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies)."

Department of the Interior, Security Control Standard, System and Information Integrity version 1.2, dated December 2012, SI-2 Flaw Remediation states:

"Control: The organization:

- a. Identifies, reports, and corrects information system flaws;
- b. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and
- c. Incorporates flaw remediation into the organizational configuration management process."

Department of the Interior, Security Control Standard, Configuration Management, version 1.2, dated December 2012, control CM-02 – Baseline Configuration states:

"Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system".

Additionally, control CM-06 – Configuration Settings states:

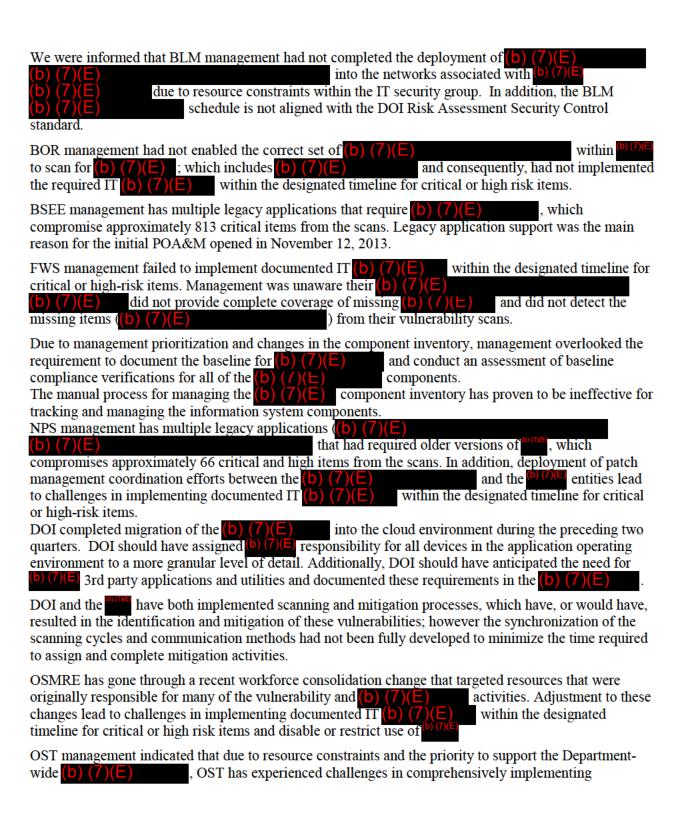
"c. Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements"

Lastly, control CM-8 – Information System Component Inventory states:

"Control: The organization develops, documents and maintains an inventory of information system components that:

a. Accurately reflects the current information system;

is consistent with the authorization boundary of the information system..."



⁶ The United States Chief Information Officer instructed Federal agencies to immediately take a number of steps to further protect Federal information and assets and improve the security of Federal networks.

documented IT (b) (7)(E within the designated timeline for critical or high risk items and disable or restrict use of USGS management originally had developed (b) (7)(E) as a test environment without production assets. As testing progressed, production assets were migrated into the environment without implementing vulnerability management capabilities. SOL management indicated that due to continued resource constraints, SOL has experienced challenges in comprehensively implementing documented IT (b) (7)(E) within the designated timeline for critical or high risk items and (b) (7)(E) were not developed and documented. Without BLM's visibility of (b) (7)(E) in the networks associated with (b) (7)(E)management processes lead to inconsistent (b) (/)(b) Inconsistent (b) (7)(E)can lead to increased risk to the DOI computing environment, which is vital to the DOI mission. The organizational risks could lead to potential inappropriate system access, system errors and potential lost or disclosure of DOI information. We recommend BLM: 1. Enhance the (b) (7)(E) for (b) (7)(E) and allocate resources to deploy (b) (7)(E) (b) (5) on the timeframe designated by the DOI standards; 2. Finalize the deployment of (b) (7)(E) within all BLM networks to provide capabilities; and 3. Ensure IT (b) (7)(E) are implemented in accordance with the DOI Risk Assessment and System and Integrity Information security control standards. We recommend BOR: procedures to include a periodic review of the (b) (7) 4. Enhance the (b) (7)(E) 5. Ensure IT (b) (7)(E) are deployed timely according to the (b) (7)(E) guidance and Department of the Interior, Security Control Standard for RA-5. We recommend BSEE: 6. Ensure IT (b) (7)(E) are implemented in accordance with the DOI Risk Assessment and System and Integrity Information security control standards; 7. Update and maintain active POA&Ms for items requiring additional time for remediation; and 8. Develop a solution for legacy application support that would allow (b) (7)(E) to be deployed to majority of the BSEE environment. Possible solutions may include one or more of the following: a. Re-development of legacy applications to support newer versions of (b) (7)(E) b. Utilization of sandbox technologies ((b) (7)(E) c. Alternative (b) (7)(E) to cover BSEE computing environment. We recommend FWS: 9. Ensure IT (b) (7)(E) are deployed timely according to (b) (7)(E) guidance and Department of the Interior, Security Control Standard for RA-5; and 10. Augment the (b) (7)(E) process with their existing vulnerability scanning tools by analyzing multiple data points to improve detection of missing (b) (7)(E) , in addition to improving oversight of System Owner remediation efforts.

We recommend NPS:

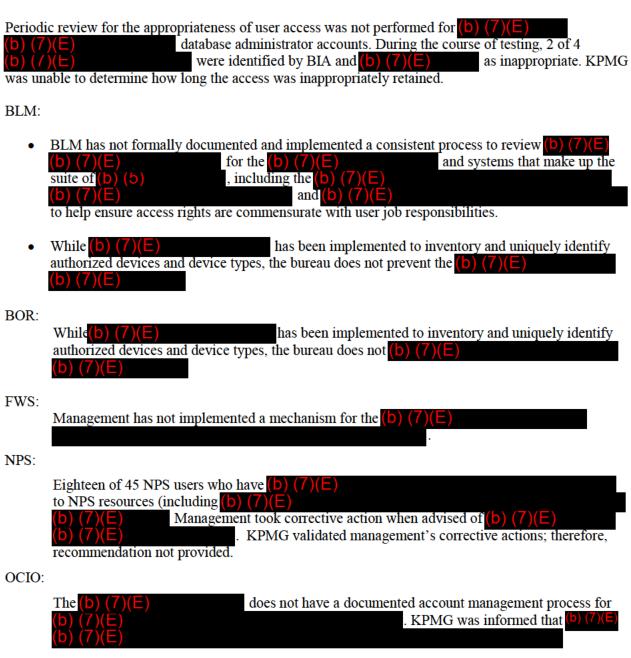
- 11. Ensure IT (b) (7)(E) are deployed timely according to (b) (7)(E) guidance and Department of the Interior, Security Control Standard for RA-5;
- 12. Update and maintain active Plan of Action and Milestones (POA&Ms) for items requiring additional time for fixes; and

13. Test and deploy newer versions of (b) (7)(E) to support recently upgraded implementation of legacy applications for compatibility. We recommend OCIO: 14. Develop and coordinate a (b) (7)(E) strategy and process that outlines responsibility of all three groups ((b) (7)(E)), coordinates the deployment of (b) (7) (E)), and maintains a vulnerability scanning process that provides oversight to the respective groups; and 15. Ensure IT (b) (7)(E) are deployed timely according to (b) (7)(E) guidance and Department of the Interior, Security Control Standard for RA-5; and 16. Disable or restrict the use of the on networked devices. We recommend OSMRE: 17. Ensure IT(b) (7)(E) are deployed timely according to the (b) (7)(E) guidance and Department of the Interior, Security Control Standard for RA-5; and 18. Disable or restrict the use of the (b) (7)(E) on networked devices. We recommend OST: 19. Ensure IT (b) (7)(E) are deployed timely according to (b) (7)(E) guidance and Department of the Interior, Security Control Standard for RA-5; and 20. Disable or restrict the use of the (b) (7)(E) on networked devices. We recommend USGS: 21. Continue corrective actions as described in POA&M (b) (7)(E) which includes continued vulnerability scanning by the contractor and Management performing remediation activities on items discovered: 22. Continue to develop and migrate the (b) (7)(E) information system into the new cloud-based environment developed under the (b) (7) (E): and program and flaw remediation processes consider cloud-23. Ensure the (b) (7)(**E**) based information systems that are part of the USGS system inventory. We recommend SOL: 24. Ensure IT (b) (7)(E) are deployed timely according to (b) (7)(E) and Department of the Interior, Security Control Standard for RA-5; and 25. Create and maintain active Plan of Action and Milestones (POA&Ms) for items requiring additional time for fixes. 26. SOL management should identify the (b) (7)(E) components operating in the SOL network environment, develop, document, and implement an agreed-upon set of baseline configurations.

3. Implementation of the Identity and Access Management Program Needs Improvement

KPMG noted the following weaknesses in 8 of 13 bureaus and offices, BIA, BLM, BOR, FWS, NPS, OCIO, OSMRE, and SOL identity and access management programs:

BIA:



OSMRE:

While OSMRE has implemented monthly reviews of OSMRE (b) (7)(E)
(b) (7)(E) accounts that are inactive for (b) (7)(E) , the system was not configured to enforce (b) (7)(E) Furthermore, the review over inactive accounts was

determined to be ineffective, as 1 of 523 active accounts (b) (7)(E)

(b) (7)(E)

SOL:

- 24 of 415 network accounts (b) (7)(E)
 (b) (7)(E)
- SOL has not developed and implemented a process for the (b) (7)(E)

Department of the Interior, Security Control Standard, Access Control (AC), version 1.4, dated December 2012, control AC-02 – Account Management states:

Applicability: All Information Systems

Control: The organization manages information system accounts, including:

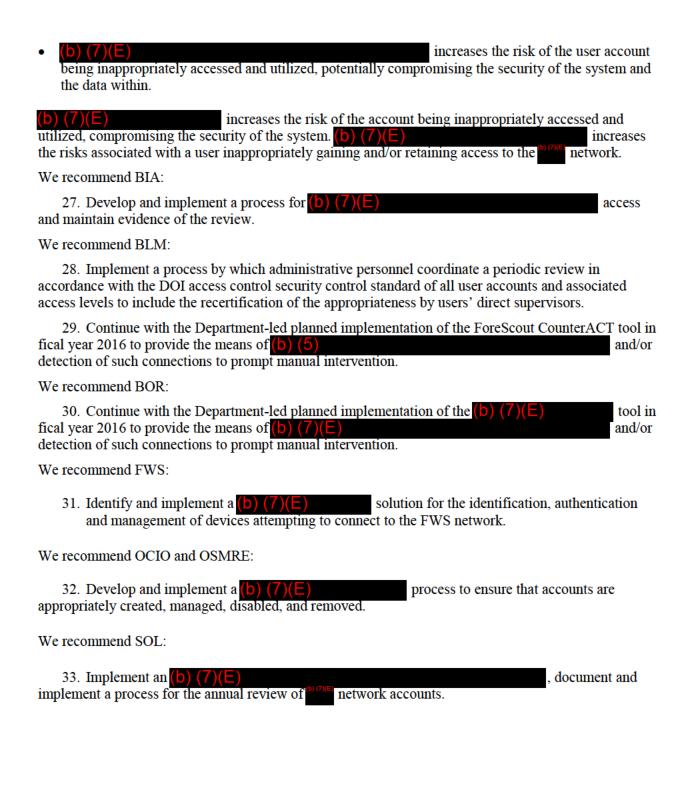
- a. Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);
- b. Establishing conditions for group membership;
- c. Identifying authorized users of the information system and specifying access privileges;
- d. Requiring appropriate approvals for requests to establish accounts;
- e. Establishing, activating, modifying, disabling, and removing accounts;
- f. Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;
- g. Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/ need-to-share changes;
- h. Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;
- i. Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and
- j. Reviewing accounts annually.

DOI Security Control Standard Identification and Authentication, Version 1.5, IA-3 Device Identification and Authentication

Applicability: Moderate and High Impact Information Systems

<u>Control</u>: The information system uniquely identifies and authenticates [Assignment: organization defined list of specific and/or types of devices] before establishing a connection.

(b) (7)(E) does perform quarterly application user account reconciliations; however, they do not have visibility into (b) (7)(E)
The need to perform a regular review of the (b) (7)(E) was not considered outside of processes in place to help ensure (b) (7)(E) . This is due to a general lack of knowledge of the need for such a control component.
The need to perform a regular review of the (b) (7)(E) was not considered. This is due to a general lack of knowledge of the need for such a control component.
BLM management has not completed implementation activities related to the department-supported (b) (7)(E) , which will enable the (b) (7)(E) of undefined devices attempting to connect to the network.
BOR management has not completed implementation activities related to the department-supported (b) (7)(E) , which will enable the (b) (7)(E) of undefined devices attempting to connect to the network.
As a result of management prioritization, FWS failed to define and implement (b) (7)(E) (b) (7)(E)
NPS had not provided sufficient oversight to enforce and monitor compliance with Department and NIST Identity and Access Management policies.
OCIO management did not implement a solution for (b) $(7)(E)$ to meet account management needs. Furthermore, the (b) $(7)(E)$ for removing accounts for terminated users is (b) $(7)(E)$
SOL has implemented a (b) $(7)(E)$ accounts that has proven to be ineffective in ensuring that (b) $(7)(E)$. Additionally, due to operational prioritization, a process for the periodic review of network accounts has (b) $(7)(E)$
The lack of a periodic review of (b) $(7)(E)$ access increases the risks associated with users inappropriately gaining and/or retaining privileged access to (b) $(7)(E)$
By not performing a (b) (7)(E) on a regular basis, employees and contractors may have access to the system that is outside the realm of the job responsibilities.
This (b) (7)(E) allow a person to advertently or inadvertently use system functions to alter the integrity of system data.
A lack of (b) (7)(E) could lead to the addition of unauthorized hardware connections to the bureau network and expose information technology resources to unforeseen vulnerabilities, attacks, or inappropriate use of network resources.
Not implementing a (b) (7)(E) solution leaves FWS vulnerable to the risks associated with connecting to the environment. It also leaves FWS susceptible to the risks associated with authorized devices connecting to the network without (b) (7)(E).
(b) (7)(E) increases the risk of the account being inappropriately accessed and utilized, potentially compromising the security of the system and the data stored.
KPMG noted the following effects for the OCIO exceptions noted above:
• (b) (7)(E) hinders management from ensuring that system processes are implemented in compliance with applicable Department and federal requirements.
• (b) (7)(E) of user accounts increases the risk of a user inappropriately obtaining access and privileges, potentially compromising the security of the system.



4. Implementation of the Incident Response and Reporting Program Needs Improvement KPMG noted the following weaknesses in 4 of 13 bureaus and offices, BLM, BOR, OCIO, and SOL incident response and reporting programs:

BLM, BOR, and SOL:

While information system audit logging is enabled there (b) (7)(E)

OCIO:

- KPMG inspected the DOI Computer Security Incident Response Handbook, version 4.0, dated November 13, 2014 and determined that updates are required. The Department is working to update procedures and disseminate to the bureaus and offices when complete. Specifically, the handbook requires updates to the following sections:
 - 5.0 Threat Assessment: Threat levels, such as high, medium, low, and none, used to determine the seriousness of an incident, including triggers, scope, and risk imposed.

	HIGH – Organization has lost the ability to provide all critical services to
	all system users.
	MEDIUM – Organization has lost the ability to provide a critical service
Functional	to a subset of system users.
Impact	LOW – Organization has experienced a loss of efficiency, but can still
1 *	provide all critical services to all users with minimal effect on
	performance.
	NONE – Organization has experienced no loss in ability to provide all
	services to all users.

• 6.0 Reporting: Determine and incorporate information impact and recovery information beyond Privacy (PII) and Regular recoverability timelines.

	CLASSIFIED – The confidentiality of classified information was
	compromised.
	PROPRIETARY – The confidentiality of unclassified proprietary
	information, such as protected critical infrastructure information
	(PCII), intellectual property, or trade secrets was compromised.
Information	PRIVACY – The confidentiality of personally identifiable
Impact	information (PII) or personal health information (PHI) was
	compromised.
	INTEGRITY – The necessary integrity of information was modified
	without authorization.
	NONE – No information was exfiltrated, modified, deleted, or
	otherwise compromised.
	REGULAR – Time to recovery is predictable with existing
	resources.
	SUPPLEMENTED – Time to recovery is predictable with additional
	resources.
Recoverability	EXTENDED – Time to recovery is unpredictable; additional
	resources and outside help are needed.
	NOT RECOVERABLE – Recovery from the incident is not possible
	(e.g., sensitive data exfiltrated and posted publicly).
	NOT APPLICABLE – Incident does not require recovery.

• Appendix A – DOI Incident Report Form: Ability to document the Functional Impact (High, Medium, Low, None), Information Impact (Classified, Proprietary, Privacy, Integrity, None), and Recoverability (Regular, Supplemented, Extended, Not Recoverable, Not Applicable).

DOI Security Control Standard Audit and Accountability, Version: 1.2, AU-6 Audit Review, Analysis, and Reporting.

Applicability: All Information Systems

Control: The organization develops, disseminates, and reviews/updates annually:

- a. Reviews and analyzes information system audit records at least weekly for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and
- b. Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information.

Department of the Interior, Security Control Standard, Incident Response (IR) version 1.2, dated December 2012, control IR-1 Incident Response Policies and Procedures states:

"Control: The organization develops, disseminates, and reviews/updates at least annually:

- a. A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls."

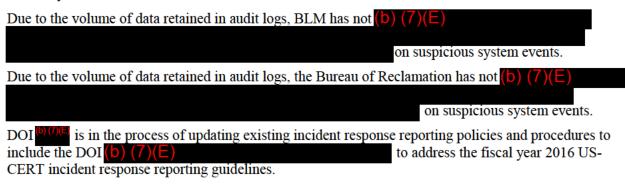
Department of the Interior, Security Control Standard, Incident Response (IR) version 1.2, dated December 2012, control IR-6 – Incident Reporting states:

"Control: The organization:

- a. Requires personnel to report suspected security incidents to the organizational incident response capability within US-CERT incident reporting timelines as specified in NIST Special Publication 800-61 (as amended); and
- b. Reports security incident information to designated authorities".

The Office of Management and Budget memorandum M-07-16 – *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007 states:

"Agencies must report all incidents involving personally identifiable information [PII] to US-CERT. This reporting requirement does not distinguish between potential and confirmed breaches. The US-CERT concept of operations for reporting Category 1 incidents is modified as follows: Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information. In this category agencies must report when there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred. Reporting to US-CERT is required within one hour of discovery/detection".



Documented system attacks or data loss may go unnoticed and continue to occur if audit trail data is reviewed and acted upon on a regular basis.

Failure to implement may lead to delays in resolving incidents or prevent correlating an incident within the expected timeframe and holding responsible individuals fully accountable.

We recommend BLM:

- 34. Identify and define key events that represent moderate to significant risks to the operation and availability of (b) (7)(E); and
- 35. Assign the ISSO, or other security personnel, the responsibility of formally documenting and reviewing events and researching the nature of suspicious activity for root cause, risk mitigation, and trends on a weekly basis as defined by department policy.

We recommend BOR:

- 36. Identify and define key events that represent moderate to significant risks to the operation and availability of (b) (7)(E); and
- 37. Assign the ISSO, or other security personnel, the responsibility of formally documenting and reviewing events and researching the nature of suspicious activity for root cause, risk mitigation, and trends on a weekly basis as defined by department policy.

We recommend SOL:

- 38. Identify and document auditable events and activities that should be monitored on (b) (7)(E)
- 39. Develop and implement a process to ensure (b) (7)(E) are reviewed and analyzed for inappropriate and/or unusual activity, in accordance with the DOI Audit and Accountability Security Control Standard.

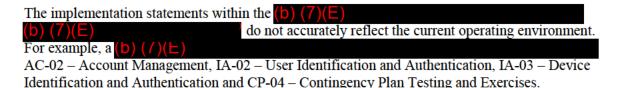
We recommend OCIO:

- 40. Continue updating incident response policies and procedures, to include the incident response security control standard and incident response handbook in accordance with NIST Special Publication 800-61 revision 2 and US-CERT federal incident notification guidelines.
- 41. Disseminate updated and approved incident response policies and procedures to all bureau and offices.
- 42. Establish a timeline for bureaus and offices to fully implement updated incident response policies and procedures.

5. Implementation of the Risk Management Program Needs Improvement

KPMG noted the following weaknesses at 3 of 13 bureaus and offices, BIA, FWS, and SOL risk management programs:

BIA:



FWS:

- FWS management inappropriately continued operation of the pilot initiative for the (b) (7)(E), which was not appropriately authorized through the (b) (7)(E) for authorization to operate. (b) (7)(E) operated without an Authorization to Operate (ATO).
- (b) (7)(E) security management has not fully developed and documented implementation statements in the (b) (7)(E) for the applicable security controls. For example, an (b) (7)(E) documented for controls AC-02 Account Management, CM-02 Baseline Configuration and CP-09 Information System Backup.

SOL:

The implementation statements within the (b) (7)(E) do not accurately reflect the current operating environment. For example, the (b) (7)(E) accurate for controls IA-02 – User Identification and Authentication, AU-02 – Auditable Events and CP-09 – Information System Backup.

Department of the Interior, Security Control Standard, Planning, version 1.2, dated December 2012, control PL-2 – System Security Plan states:

"Control: The organization:

a. Develops a security plan for the information system that...Describes the security controls in place or planned for meeting those requirement including a rationale for the tailoring and supplementation decisions..."

Department of the Interior, Security Control Standard, Security Assessment and Authorization (CA) version 1.3, dated December 2012, control CA-6 – Security Authorization states:

"Control: The organization:

b. Ensures that the authorizing official authorizes the information system for processing before commencing operations...

BIA management had not provided adequate oversight and support to the (b) (7)(E) to ensure that system security plan documentation is accurate and up-to-date.

FWS management failed to formally authorize the information system at the end of the authorized pilot period in 2012.

FWS management has not provided adequate oversight and support to the (b) (7)(E) for ensuring that system security plan documentation is accurate and up-to-date.

SOL has contracted the services of the Office of the Chief Information Officer (OCIO) for the facilitation and completion of the (b) (7)(E). Due to competing priorities and resource constraints, the SSP was not reviewed and updated as part of the risk management framework process for (b) (7)(E) at the beginning of fiscal year 2015.

Lack of implementation description of security controls hinders authoring official's, and other BIA security management, the ability to assess and ensure the information system's compliance with the relevant security control requirements.

Not properly authorizing an information system for operation exposes the FWS environment to risks to the organization operations and assets, individuals, other organizations and the Nation. Lack of implementation description of security controls hinders authoring officials, and other FWS security management, the ability to assess and ensure the information system's compliance with the relevant security control requirements.

We recommend BIA:

43. BIA management should continue to work with (b) (7)(E) to ensure that the SSP is complete and accurate; including verifying the accuracy of the implementation statements for controls AC-02, IA-02, IA-03 and CP-04.

We recommend FWS:

- 44. Ensure all production information systems follow the NIST SP 800-37 Risk Management Framework to include authorization.
- 45. Enforce the requirement to ensure that the (b) (7)(E) is complete and accurate, including documenting implementation statements.

We recommend the SOL:

46. Coordinate with SOL management to ensure that the (b) (7)(E) is complete and accurate including documenting implementation statements for controls IA-02, AU-02 and CP-09.

6. Implementation of the Security Training Program Needs Improvement

KPMG noted the follow weaknesses in 2 of 13 bureaus and offices, BIA and USGS security training programs:

BIA:

KPMG determined that the BIA Authorizing Official (AO) and 3 of 5 National Irrigation
(b) (7)(E) did not completed the required role-based security training (RBST) courses for Fiscal Year 2015.

USGS:

- USGS did not appropriately disable 4 of 15 USGS (b) (7)(E) who did not complete the fiscal year 2015 Federal Information System Security Awareness (FISSA+) training.
- 8 of 11 (b) (7)(E) did not complete role-based security training (RBST) for fiscal year 2015.

Department of the Interior, Security Control Standard, Awareness and Training (AT), version 1.2, dated December 2012, control AT-02 – Security Awareness states:

"The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and annually thereafter".

Additionally, control AT-03 – Security Training states:

"The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) at least annually thereafter".

Department of the Interior Role-Based Security Training (RBST) Standard, version 2.6.0, dated March 11, 2011, pages 6-7 document that AOs are part of RBST Group 1 – Executive and Senior Management. RBST should include at least 1 of the following topic areas:

- Information Security Basics
- Policy Level Security Planning and Management
- Emergency Management and Disaster Recovery
- Strategic Security Planning or Implementation
- Risk Management Framework

Additionally, pages 8-9 document that CISOs and system administrators are part of RBST Group 3 – Information Security Personnel. RBST should include at least 2 of the following information security training focus areas:

- Information Security Basics
- Security Planning
- System/Application Security Management
- System Application Life Cycle Management
- Risk Management
- Contingency Planning
- Incident Response
- Account Management and Access Controls
- Configuration Management and Change Control
- Data Classification and Records Management

BIA misinterpreted the DOI requirements for the number of RBST courses required for each training group. This resulted in personnel with significant security responsibility not appropriately completing their FY15 RBST requirements.

USGS has not developed an effective process for reconciling DOI Learn to the network user population to ensure that users who do not complete annual FISSA+ training are disabled, and remain disabled until the training is completed. In addition, USGS has not developed an effective process to ensure that all users with significant security responsibility, such as system administrators for the USGS information systems, are correctly assigned RBST.

Lack of security training and RBST increases the risks associated with users, with access to DOI resources and information, not understanding their information security responsibilities, Departmental policies, and how to properly protect information resources entrusted to them.

We recommend BIA:

47. Enhance the current Indian Affairs RBST process to ensure that users with significant security responsibilities are identified, are aware of their training requirements, and are reminded that individuals are responsible for maintaining evidence of their training in accordance with the DOI RBST Standard.

We recommend USGS:

- 48. Enforce the current process for ensuring that the (b) (7)(E) for users who do not complete the annual security training are disabled until the requirement is met.
- 49. Enhance the current process for ensuring that all personnel with significant information security to include system administrator responsibilities are identified and appropriately assigned RBST in the DOI Learn system.

7. Implementation of the Plan of Action and Milestones Program Needs Improvement

KPMG noted the following weaknesses in 1 of 13 bureaus and offices, FWS plan of action and milestone program.

During the course of testing, KPMG identified two FWS program-level Plan of Action and Milestones (POA&Ms) that are not effectively tracked and remediated. Specifically:

- FWS Program POA&M # regarding the lack of implementation for control CA-7 Continuous Monitoring, was not consistently reviewed and updated on a quarterly basis in FY15.
- FWS Program POA&M # for control PM-11 Mission/Business Process Definition, regarding IT considerations having not been integrated into business process development, evidence of review or update by management this fiscal year. Additionally, KPMG noted that significant progress has not been made towards the remediation of this POA&M since its creation in 2011.

Department of the Interior, Security Control Standard, Security Assessment and Authorization (CA) version 1.3, dated December 2012, control CA-05 – Plan of Actions and Milestones states:

"Control: The organization:

b. Updates existing plan of action and milestones at least quarterly based on the findings from security control assessments, security impact analyses, and continuous monitoring activities.

FWS management failed to consistently review or update all open POA&Ms.

By not properly monitoring the status of POA&Ms, FWS management may not be adequately aware of the security weaknesses associated with the outstanding POA&Ms. In addition, management may not be aware of POA&M delays such as the allocation of the appropriate resources necessary to mitigate the current weaknesses. Lastly, POA&Ms not remediated within a timely manner increases FWS' susceptibility to the risks.

We recommend that FWS:

50. Enforce the current process and provide information system support, for the management, oversight and remediation of POA&Ms.

8. Implementation of the Contingency Planning Program Needs Improvement

KPMG noted the following weaknesses 5 of 13 bureaus and offices, BIA, BLM, BOR, FWS, and SOL contingency planning programs.

BIA:

- The BIA Continuity of Operations Plan (COOP) does not include business considerations for mission essential functions and the continuity of BIA operations outside of information technology (IT) functionality.
- BIA was unable to provide evidence of the FY15 COOP exercise. As such, KPMG could not
 determine whether the exercise was performed and was executed in compliance with Federal
 Information Security Management Act (FISMA) requirements, Federal Continuity Directives
 (FCD) and applicable National Institute of Standards and Technology (NIST) guidelines.

BLM:

The BLM Network Operations Center Contingency Plan was not tested within the last year to help ensure the recoverability and continuity of functions, operations, and resources related to (b) (7)(E)

 We were informed that due to recent organizational changes contingency recovery team members are not aware of their roles and responsibilities.

BOR:

• KPMG judgmentally selected 25 (b) (7)(E) daily backups and determined that 7 of 25 daily backups selected did not complete successfully and were not resolved in one day in accordance with backup procedures. One of seven failed backups was resolved within two days while the remaining six failures went unresolved for periods ranging from three to 14 days.

FWS:

• KPMG judgmentally selected 15 of 91 (b) (7)(E) and determined for 2 of 15 servers (b) (7)(E), management was unable to provide evidence that information system backups were conducted in accordance with the DOI Security Control Standard requirements. KPMG was unable to determine the occurrence of the last successful backup for these servers.

SOL:

- SOL was unable to provide the COOP to the KPMG FISMA team for inspection.
- (b) (7)(E) contingency planning and business continuity were not tested in FY15.
- (b) (7)(E) backups are not configured to execute in accordance with DOI requirements. Specifically, full information system backups are not configured to occur weekly and incremental information system backups are not configured to occur daily.

Federal Continuity Directive 1 (FCD-1), Annex D-Essential Functions, dated October 2012, states: Requirements for Essential Functions:

1. Organizations must identify and prioritize their essential functions, using the methodology outlined in FCD 2, and document them in its continuity plan. These essential functions serve as the framework for the continuity plan and organizations should account for all continuity capabilities required for the performance essential functions.

- 3. Organizations must conduct a [Business Process Analysis] BPA to determine the essential functions that they must perform under all circumstances either uninterrupted, with minimal interruption, or requiring immediate execution in an emergency.
 - a. The BPA must identify and map the functional processes, workflows, activities, resources, personnel expertise, supplies, equipment, infrastructures, systems, data, and facilities inherent to the execution of each identified essential function.
 - b. The organization head or designee must validate and approve the identified essential functions and BPA.
- 4. Organizations must conduct a business-process flow map to identify how each essential function is performed and executed.

Additionally, FCD-1, Annex K – Test, Training and Exercise (TT&E) Program states that the COOP must be tested annually. It also states "As part of its TT&E program, the organization must document all conducted TT&E events, including documenting the date of the event, those participating in the event, and the results of the event".

DOI Security Control Standard Contingency Planning, Version 1.3, CP-4 Contingency Plan Testing and Exercises

Applicability: All Systems

<u>Control</u>: The organization:

- A) Tests and/or exercises the contingency plan for the information system at least annually using functional exercise for moderate impact systems; classroom exercise/table top written tests for low impact systems to determine the plan's effectiveness and the organization's readiness to execute the plan; and
- B) Reviews the contingency plan test/exercise results and initiates corrective action.

DOI Security Control Standard Contingency Planning, Version: 1.3, December 2012, CP-9 Information System Backup

Applicability: All Information Systems

Control: The organization:

- a. Conducts backups of user-level information contained in the information system at least daily incremental and weekly full;
- b. Conducts backups of system-level information contained in the information system at least daily incremental and weekly full;
- c. Conducts backups of information system documentation including security-related documentation at least daily incremental and weekly full; and
- d. Protects the confidentiality and integrity of backup information at the storage location.

BIA has not coordinated with business management to incorporate and integrate business considerations into the BIA COOP. In regards to the annual COOP exercise, test plans, results and lessons learned were not appropriately documented in coordination with the completion of the exercise. The BIA COOP document was incomplete and BIA (b) (7)(E) in fiscal year 2015.

BLM management has not placed attention on testing the NOC Contingency Plan. Recent reorganizations, a lack of identified and properly trained resources, and a lack of a designated contingency site to perform testing are contributing factors.

BOR management relies on automated job runs on the following business day to resolve failures and there is not a formalized process requiring manual intervention in rectifying (b) (7)(E)

Because of FWS management's inability to maintain a listing of the system components inventories, the implementation of information system backups for (b) (7)(E) was not consistently applied.

KPMG noted the following causes for the SOL conditions noted above:

- SOL management relied on the Office of the Chief Information Officer (OCIO) for COOP development, which resulted in the lack of development of a SOL COOP.
- Due to operational prioritization the SOL contingency plan (b) (7)(E)
- A misinterpretation of DOI requirements resulted in the SOL information system backups not being conducted at the appropriate frequency.

Not including business considerations in the COOP leaves BIA susceptible to the risk of loss of business functionality in the event of a disruption of operations. Additionally, BIA cannot ensure that continuity of IT functionality, meant to support business missions, is sufficient to support the business recovery needs of the Bureau. Not performing an annual exercise of the COOP will hinder BIA from ensuring that the COOP, as designed, is sufficient to support the reconstitution of operations in the event of a disruption.

Without testing the BLM NOC Contingency Plan and system fail-over capability, deficiencies in the plan and the system fail-over capability may not be identified and addressed. As a result, in the event of a disaster, the NOC Contingency Plan may not be adequate to continue essential BLM activities. Failure to adequately train staff in their Contingency Plan roles and responsibilities increases the risk of system recovery delays due to poor coordination or understanding of responsibilities.

Without a process to actively monitor the status of backup jobs, there is the risk of loss of data that may result in operating inefficiencies and disruption of operations in the event of system failure or a disaster.

Without functioning backups and/or replication, data to continue FWS operations may not be available if was to become inoperable or lost.

Not developing and documenting a COOP leaves SOL susceptible to the risk of loss of business and information technology functionality in the event of a disruption of operations. Not performing an annual exercise of the COOP and information system contingency plan will hinder SOL from ensuring that the COOP, as designed, is sufficient to support the reconstitution of operations in the event of a disruption. Lastly, without frequent backups and/or replication, data to continue SOL operations may not be available if the network was to become inoperable or lost.

We recommend BIA:

- 51. Coordinate with business management to enhance the mission essential functions for the COOP.
- 52. Ensure that the COOP is tested on an annual basis and the test plan and results are appropriately documented and maintained.

We recommend BLM:

- 53. Test the NOC Contingency Plan in accordance with NIST requirements. The test documentation should indicate the methodology, procedures, results, and lessons learned. Where necessary, the NOC Contingency Plan should be updated based on the results of the test.
- 54. Train recovery team members on their system recovery roles and responsibilities.

We recommend BOR:

55. Design and implement a process in which the status of backups jobs are reviewed help ensure unsuccessful backups are manually resolved when not automatically rerun to success the following

37

We recommend FWS:

56. Follow the existing process to ensure that information system components are appropriately identified and backups are consistently performed, in accordance with Departmental policy, for all servers.

We recommend SOL:

- 57. Develop and document a COOP in accordance with the requirements documented in FCD-1.
- 58. Enforce the requirement to test the (b) (7)(E) contingency plans at least annually.
- 59. Update and enforce information system backup procedures to ensure backups are performed in accordance with control CP-09 of the DOI Contingency Planning Security Control Standard.

Conclusion

As part of the FISMA performance audit of the subset of DOI information systems, we assessed the effectiveness of the Department's information security program and practices and the implementation of the security controls in NIST SP 800-53 Revision 3. We identified needed improvements in most areas audited including continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, plan of action and milestone, remote access management, and contingency planning.

Management Response to Report

to deploy (b) (7)(E) on the timeframe designated by the DOI standards." Management Response: Concur. Existing POA&Ms (b) (7) have been updated with the FYI 5 finding notes. The overall vulnerability posture has greatly improved. However, BLM will ensure that (b) (7)(E) have been installed and are reporting correctly on all (b) (7)(E)systems and will review patch management procedures to align with DOI standards. Recommendation 2: BLM: "Finalize the deployment of (b) (7)(E) within all BLM networks to provide patch management and vulnerability management capabilities." Management Response: Concur. The existing POA&Ms (b) (7)(E)) have been updated with the FYI 5 finding notes. The overall vulnerability posture has greatly improved. However, BLM will ensure that (b)(7)(E)have been installed and are reporting correctly on all (b) (7)(E)and will review patch management procedures to align with DOI standards. Recommendation 3: BLM: "Ensure IT (b) (7)(E) are implemented in accordance with the DOI Risk Assessment and System and Integrity Information security control standards. Management Response: Concur. The existing POA&Ms ((b) (7)(E)) have been updated with the FYI 5 finding notes. The overall vulnerability posture has greatly improved. However, BLM will ensure that (b)(7)(E)have been installed and reporting correctly on all (b) (7)(E) and will review patch management procedures to align with DOI standards. Recommendation 4: BOR: "Enhance the vulnerability management procedures to include a periodic review of the (b) (7)(E) settings." Management Response: Concur. The BOR Vulnerability Management Procedure has been updated to include a periodic review of the (b) (7)(E) settings. Recommendation 5: BOR: "Ensure IT (b) (7)(E) are deployed timely to the patch management guidance and Department of the Interior, Security Control Standard for RA-S." are being deployed more timely, partly in response Management Response: Concur. (b) (7)(E) to the Cybersecurity Sprint, and according to DOI guidance. BOR has reduced the number of critical vulnerabilities by 80% over the last two months. The average number of vulnerabilities per machine went from 26 to 11. Additionally, all identified (b) (7)(E) servers have had the latest patch applied. Recommendation 6: BSEE: "Ensure IT (b) (7)(E) are implemented in accordance with the DOI Risk Assessment and System and Integrity security control standards." Management Response: Concur. BSEE will continue to expand their efforts to ensure patches and security advisories are addressed upon dissemination by US-CERT or discovery through vulnerability assessment tools. Numerous improvements to the patching process and tools have already been implemented and continue to be fine-tuned to assure compliance with DOI Risk Assessment and System and Integrity Information security control standards. Process enhancements include leveraging pre-approved changes and accelerated testing for operating system security patches, as well as certain third party applications, to expedite remediation of critical security advisories. Patch management system enhancements have improved (b) (7)(=) performance through restructuring of deployment packages and modification of . These improvements have already contributed to BSEE/QNRR lowering their average number of

Recommendation 1: BLM: "Enhance the patch management schedules for (b) (7)(E) and allocate resources

vulnerabilities on a per system basis. BSEE will also evaluate other patch management tools, such as (b) (7)(E) as alternatives to further improve patch management within the BSEE environment.

Recommendation 7: BSEE: "Update and maintain active POA&Ms for items requiring additional time for remediation."

Management Response: Concur. BSEE will reassess our POA&M update and maintenance process and the roles responsible for monitoring them and define a strategy for items requiring additional time for fixes.

Recommendation 8: BSEE: "Develop a solution for legacy application support that would allow security fixes to be deployed to majority of the BSEE environment. Possible solutions may include one or more of the following:

- a. Re-development of legacy applications to support newer versions of (b) (7)(E).
- b. Utilization of sandbox technologies ((b) (7)(E)
 (b) (7)(E)).
- c. Alternative patching strategies to cover majority of BSEE environment."

Management Response: Concur. BSEE will engage with BSEE, BOEM and ONRR representatives to review solution alternatives, which enable deployment of security fixes to the majority of the BSEE environment. BSEE is already demonstrating progress towards this recommendation. An upgrade and re-platforming of the legacy (b) (7)(E) was initiated in FY15 and is expected to be complete in FY16. We anticipate these system improvements will reduce the number of longstanding vulnerabilities and better position the Bureau for adhering to a regular patch management schedule. A balanced strategy will be devised for remaining legacy systems and application support that meets Mission area needs and protects BSEE's security posture.

Recommendation 9: FWS: "Ensure IT software security patches are deployed timely according to patch management guidance and Department of the Interior, Security Control Standard for RA-5."

Management Response: Concur. The FWS created POA&M in the (b) (7)(E)

FWS management will ensure IT software security patches are deployed timely according to patch management guidance and Department of the Interior, Security Control Standard for Risk Assessment RA-5 Vulnerability Scanning.

Recommendation 10: FWS: "Augment the patch management process with their existing vulnerability scanning tools by analyzing multiple data points to improve detection of missing security patches and fixes, in addition to improving oversight of System Owner remediation efforts."

Management Response: Concur. The FWS created POA&M in the (b) (7)(E)

FWS management will augment the patch management process with their existing vulnerability scanning tools by analyzing multiple data points to improve detection of missing security patches and fixes, in addition to improving oversight of System Owner remediation efforts.

Recommendation 11: NPS: "Ensure IT software security patches are deployed timely according to patch management guidance and Department of the Interior, Security Control Standard for RA-5."

Management Response: Concur. (b) (7)(E) has taken immediate action and manually applied patches to all servers. A renewed effort is underway to resolve the outstanding issue with receiving centrally deployed patches, in accordance with DOI Security Control Standard RA-5.

Recommendation 12: NPS: "Update and maintain active Plan of Action and Milestones (POA&Ms) for items requiring additional time for fixes."

Management Response: Concur. Plan of Action and Milestones (POA&Ms) are under review and will be updated accordingly.

Recommendation 13: NPS: "Test and deploy newer versions of (b) (7)(E) to support recently upgraded implementation of legacy applications for compatibility."

Management Response: Concur. (b) (7)(E) applications require very specific versions of (b) (7)(E) to function correctly. Updates have already been applied (b) (7)(E) to address more serious vulnerabilities. The remaining issues are under investigation by (b) (7)(E) support. Newer versions will be applied when compatibility is confirmed by Other older application versions are also in need of upgrade to address additional vulnerabilities.

Recommendation 14: OCIO and the Business Integration Office: "Develop and coordinate a patch management strategy and process that outlines responsibility of all three groups (b) (7)(E), coordinates the deployment of software security fixes (b) (7)(E), and maintains a vulnerability scanning process that provides oversight to the respective groups."

Management Response: Concur.

Recommendation 15: OCIO and the Business Integration Office: "Ensure IT (b) (7)(E) are deployed timely according to patch management guidance and Department of the Interior, Security Control Standard for RA-5."

Management Response: Concur.

Recommendation 16: OCIO and the Business Integration Office: "Disable or restrict the use of the on networked devices."

Management Response: Concur.

Recommendation 17: OSMRE: "Ensure IT (b) (7)(E) are deployed timely according to the patch management guidance and Department of the Interior, Security Control Standard for RA-5."

Management Response: Concur. OSMRE has since created a POA&M and is tracking (b) (7)(E) basis.

Recommendation 18: OSMRE: "Disable or restrict the use of the (b) (7)(E) on networked devices."

Management Response: Concur. Of the four identified instances of (b) (7)(E) discovered the OSMRE has disabled three and restricted the use of the fourth pending a vendor firmware update.

Recommendation 19: OST: "Ensure IT (b) (7) (E) are deployed timely according to patch management guidance and Department of the Interior, Security Control Standard for RA-5."

Management Response: Concur. OST will open a POA&M to track corrective actions.

Recommendation 20: OST: "Disable or restrict the use of the (b) (7)(E) on networked devices."

Management Response: Concur. OST will open a POA&M to track corrective actions.

Recommendation 21: USGS: "Continue corrective actions as described in POA&M which includes continued vulnerability scanning by the contractor and Management performing remediation activities on items discovered."

Management Response: Concur. Management concurs with this recommendation as documented in September 2015 USGS response to USGS-NFR-01, W/P Reference USGS-FISMA-VA-04. USGS is tracking corrective actions through POA&M (b) (7)(E) assigned to (b) (7)(E).

Recommendation 22: USGS: "Continue to develop and migrate the (b) (7)(E) into the new cloud-based environment developed under the Foundational Cloud Hosting Services contract."

Management Response: Concur. Management concurs with this recommendation as documented in September 2015 USGS response to USGS-NFR-01. USGS is tracking corrective actions through POA&M (b) (7)(E) assigned to (b) (7)(E)

Recommendation 23: USGS: "Ensure the vulnerability management program and flaw remediation processes consider (b) (7)(E) that are part of the USGS system inventory."

Management Response: Concur. Management concurs with this recommendation as documented in September 2015 USGS response to USGS-NFR-01. USGS is tracking corrective actions through POA&M (b) (7)(E)

Recommendation 24: SOL: "Ensure IT (b) (7)(E) are deployed timely according to patch management guidance and Department of the Interior, Security Control Standard for RA-5."

Management Response: Concur. SOL is reevaluating current patch deployment technology for ongoing suitability as well as exploring the possible use of (b) (7)(E) for ongoing deployments. SOL will create a POA&M for tracking.

Recommendation 25: SOL: "Create and maintain active Plan of Action and Milestones (POA&Ms) for items requiring additional time for fixes."

Management Response: Concur. SOL has partnered with the OCIO (b) (7)(E), (b) (7)(E)) group for POA&M support. Going forward, this process will be managed in collaboration with the (b) (7)(E) group. SOL will a create POA&M for tracking.

Recommendation 26: SOL: "SOL management should identify the (b) (7)(E) components operating in the (b) (7)(E) environment, develop, document, and implement an agreed-upon set of baseline configurations."

Management Response: Concur. SOL utilizes security appliances based on the (b) (7)(E). SOL is in the process of documenting the baseline configuration for these devices. SOL will create a POA&M for tracking.

Recommendation 27: BIA: "Develop and implement a process for the periodic review of (b) (7)(E) access and maintain evidence of the review."

Management Response: Concur. The implementation of (b) (7)(E) (b) (5) will facilitate the completion of this recommendation.

Recommendation. 28: BLM: "Implement a process by which administrative personnel coordinate a periodic review in accordance with the DOI access control security control standard of all user accounts and associated access levels to include the recertification of the appropriateness by users' direct supervisors."

Management Response: Concur. This recommendation will be tracked through a new POA&M in The BLM (b) (7)(E) group will work with the Project Managers and User Representatives to develop a process for account reviews, create a standard operating procedure document, and ensure each application is performing them on a defined schedule.

Recommendation 29: BLM: "Continue with the Department-led planned implementation of the (b) (7)(E) tool in fiscal year 2016 to provide the means of automated prevention of unauthorized device connections and/or detection of such connections to prompt manual intervention."

Management Response: Concur. BLM is working with DOI in this effort. A deployment date has not been identified.

Recommendation 30: BOR: "Continue with the Department-led planned implementation of the (b) (7)(E) tool in fiscal year 2016 to provide the means of automated prevention of unauthorized device connections and/or detection of such connections to prompt manual intervention."

Management Response: Concur. BOR is continuing with the Department led planned implementation of the (b) (7)(E) tool. No additional corrective actions are planned. DOI POA&M
(b) (7)(E) exists to address this.

Recommendation 31: FWS: "Identify and implement a network access control solution for the identification, authentication and management of devices attempting to connect to the FWS network."

Management Response: Concur. The FWS has existing POA&M (b) (7)(E) in the (b) (7)(E) boundary. The FWS is in the process of installing network tools called Forescout that is part of the DOI continuous monitoring initiative. Forescout uses (b) (7)(E) polling to view and catalog every device that is connected to the network. DOI has indicated that (b) (7)(E) may be integrated with (b) (7)(E) to easily authorize and deny any device that is placed on the network. Forescout will allow visibility on systems in approximately (b) (7)(E) connected to the network. Currently, (b) (7)(E) is in the discovery phase and is scheduled to deploy during FY 2016.

Recommendation 32: OCIO: "Develop and implement a formal account management process to ensure that accounts are appropriately created, managed, disabled, and removed."

Management Response: Concur.

Recommendation 33: SOL: "Implement an automated solution for disabling network accounts after document and implement a process for the annual review of (b) (7)(E) accounts."

Management Response: Concur. The policy and procedure for annual review will be updated as part the (b) (7)(E) and policy update activities currently underway. SOL has identified a technology solution for automating account maintenance. SOL will procure and implement a solution during FY16 Q2. SOL will create a POA&M for tracking.

Recommendation 34: BLM: "Identify and define key events that represent moderate to significant risks to the operation and availability of (b) (7) (E) data."

Management Response: Concur. The recommendation will be tracked through a new POA&M in (b) (7)(E) BLM has logs from (b) (7)(E) available that are parsed out by system but the (b) (7)(E) is not installed and configured on all (b) (7)(E) systems. BLM will pursue getting (b) (7)(E) installed on (b) (7)(E) systems, identify key events, and assign personnel to formally document and review events. The process, roles, and responsibilities will be documented in a standard operating procedure.

Recommendation 35: BLM: "Assign the ISSO, or other security personnel, the responsibility of formally documenting and reviewing events and researching the nature of suspicious activity for root cause, risk mitigation, and trends on a weekly basis as defined by department policy." Management Response:

Recommendation 36: BOR: "Identify and define key events that represent moderate to significant risks to the operation and availability of (b) (7)(E) data."

Management Response: Concur. A POA&M will be created to address the audit log review process and examining logs for indications of inappropriate or unusual activity.

Recommendation 37: BOR: "Assign the ISSO, or other security personnel, the responsibility of formally documenting and reviewing events and researching the nature of suspicious activity for root cause, risk mitigation, and trends on a weekly basis as defined by department policy."

Management Response: Concur. A POA&M will be created to address the audit log review process and examining logs for indications of inappropriate or unusual activity.

Recommendation 38: SOL: "Identify and document auditable events and activities that should be monitored on (b) (7)(E)."

Management Response: Concur. SOL will create a POA&M for tracking.

Recommendation 39: SOL: "Develop and implement a process to ensure (b) (7)(E)

(b) (7)(E) are reviewed and analyzed for inappropriate and/or unusual activity, in accordance with the DOI Audit and Accountability Security Control Standard."

Management Response: Concur. SOL is evaluating (b) (7)(E)
(b) (7)(E) that will correlate audit logs and facilitate efficient analysis of potential nefarious activities. SOL will also explore collaborative opportunities with (b) (7)(E) . SOL will create a POA&M for tracking.

Recommendation 40: OCIO: "Continue updating incident response policies and procedures, to include the incident response security control standard and incident response handbook in accordance with NIST Special Publication 800-61 revision 2 and US-CERT federal incident notification guidelines."

Management Response: Concur.

Recommendation 41: OCIO: "Disseminate updated and approved incident response policies and procedures to all bureau and offices."

Management Response: Concur.

Recommendation 42: OCIO: "Establish a timeline for bureaus and offices to fully implement updated incident response policies and procedures."

Management Response: Concur.

Recommendation 43: BIA: "BIA management should continue to work with (b) (7)(E) personnel to ensure that the (b) (7)(E) complete and accurate; including verifying the accuracy of the implementation statements for controls AC-02, IA-02, IA-03 and CP-04."

Management Response: Concur.

Recommendation 44: FWS: "Ensure all production information systems follow the NIST SP 800-37 Risk Management Framework."

Management Response: Concur. The FWS created POA&M (b) (7)(E) boundary. The use of (b) (7)(E) remote access platform was discontinued within the FWS before the OIG initiated its FY

2015 FISMA audit. FWS (b) (7)(E)) has allocated resources for (b) (7)(E) to undergo the (b) (7)(E) process. At the conclusion of the process, the (b) (7)(E) solution will operate with an (b) (7)(E)).

Recommendation 45: FWS: "Enforce the requirement to ensure that the (b) (7)(E) is complete and accurate, including documenting implementation statements."

Management Response: Concur. The FWS created POA&M (b) (7)(E) in the (b) (7)(E) boundary. FWS IT Security is modifying control inheritance for (b) (7)(E) The security team will document appropriate implementation statements after the modification.

Recommendation 46: OCIO: "Coordinate with SOL management to ensure that the (b) (7)(E) is complete and accurate including documenting implementation statements for controls IA- 02, AU-02 and CP-09."

Management Response: Concur.

Recommendation 47: BIA: "Enhance the current Indian Affairs RBST process to ensure that users with significant security responsibilities are identified, are aware of their training requirements, and are reminded that individuals are responsible for maintaining evidence of their training in accordance with the DOI RBST Standard."

Management Response: Concur.

Recommendation 48: USGS: "Enhance and enforce the current process for ensuring that the active directory network accounts for users who do not complete the annual security training are disabled until the requirement is met."

Management Response: Concur. Management concurs with this recommendation as documented in October 2015 USGS response to USGS-NFR-03. USGS is tracking corrective actions through POA&M (b) (7)(E) assigned to USGS Program.

Recommendation 49: USGS: "Enhance the current process for ensuring that all personnel with significant information security to include system administrator responsibilities are identified and appropriately assigned RBST in the (b) (7)(E)

Management Response: Concur. Management concurs with this recommendation as documented in October 2015 USGS response to USGS-NFR-03. USGS is tracking corrective actions through POA&M (D) (7)(E) assigned to USGS Program.

Recommendation 50: FWS: "Enhance the current process and provide information system support, for the management, oversight and remediation of POA&Ms."

Management Response: Concur. The FWS created POA&M outlined under the FWS Program to address necessary corrective actions.

Recommendation 51: BIA: "Coordinate with business management to enhance the mission essential functions for the COOP."

Management Response: Concur. has been without a (b) (7)(E) lead for a year, and as such, the responsibilities including COOP, were collateral for other personnel. now has a full-time employee filling this position and plans are in place to perform necessary testing.

Recommendation 52: BIA: "Ensure that the COOP is tested on an basis and the test plan and results are appropriately documented and maintained."

Management Response: Concur. has been without a (b) (7)(E) lead for a year, and as such, the responsibilities including COOP, were collateral for other personnel. now has a full-time employee filling this position and plans are in place to perform necessary testing.

Recommendation 53: BLM: "Test the NOC Contingency Plan in accordance with NIST requirements. The test documentation should indicate the methodology, procedures, results, and lessons learned. Where necessary, the NOC Contingency Plan should be updated based on the results of the test."

Management Response: Concur. This recommendation will be tracked through a new POA&M in CSAM. The (b) (7)(E) is currently in revision. Once this has been completed, the CP will be tested in accordance with NIST. The CP will be updated based on the results of the plan.

Recommendation 54: BLM: "Train recovery team members on their system recovery roles and responsibilities."

Management Response: Concur. This recommendation will be tracked through a new POA&M in will work with the Project Managers and User Representatives to develop a process for account reviews, create a standard operating procedure document, and ensure each application is performing them on a defined schedule.

Recommendation 55: BOR: "Design and implement a process in which the status of backups jobs are reviewed help ensure unsuccessful backups are manually resolved when not automatically rerun to success the following day."

Management Response: Concur. A portion of this recommendation is already in place: (b) (7)(E) are currently reviewed A POA&M will be created to address the weakness of unsuccessful backups being resolved when not automatically rerun to success the following day. The POA&M will be associated with (b) (7)(E) which maintains the responsibility for (b) (7)(E)

Recommendation 56: FWS: "Develop and implement a solution to ensure that information system components are appropriately identified and backups are consistently performed, in accordance with Departmental policy, for all (b) (7)(E)."

Management Response: Concur. The FWS created POA&M (b) (7)(E) in the (b) (7)(E)

The Information System Security Officer (ISSO) will take steps in concert with the Operations Manager to ensure that the inventory is accurate and current, per established procedures. The ISSO will also maintain artifacts of backup schedule or replication schedule for all components.

Recommendation 57: SOL: "Develop and document a COOP in accordance with the requirements documented in FCD-1."

Management Response: Concur. SOL will collaborate with (b) (7)(E), (b) (7)(E) group to develop and document the SOL COOP plan. SOL will create a POA&M for tracking.

Recommendation 58: SOL: "Enforce the requirement to test the (b) (7)(E) contingency plans at least annually."

Management Response: Concur. SOL will collaborate with (b) (7)(E) group to develop (b) (7)(E) CP plan testing. SOL will create a POA&M for tracking.

Recommendation 59: SOL: "Update and enforce information system backup procedures to ensure backups are performed in accordance with control CP-09 of the DOI Contingency Planning Security Control Standard."

Management Response: Concur. SOL will update backup procedures to be consistent with DOI CP-09 of the DOI Contingency Planning Security Control Standard. This will be done in coordination and collaboration with (b) (7)(E)

(b) (7)(E)

group. SOL will create a POA&M for tracking.

Appendix I – Summary of FISMA Program Areas

The following table summarizes the program areas in which control deficiencies were identified. It should not be used to infer program area compliance in general, and does not correlate to the overall program area assessments provided in Appendix V or responses provided for the FY2015 CyberScope Responses.

Area ⁷	BIA	BLM	BOR	BSEE	FWS	NPS	OCIO	OIG	OS	OSM RE	OST	SOL	USGS
СММ									X				
СМ		X	X	X	X	X	X		X	X	X	X	X
IAM	X	X	X		X	X	X		X	X		X	
IR		X	X				X		X			X	
RM	X				X							X	
ST	X												X
POA&M					X								
RAM									X8				
СР	X	X	X		X							X	
CS													

Legend:
X – Weakness identified in FISMA Program Area

48

⁷ Continuous Monitoring Management, Configuration Management, Identity and Access Management, Incident Response, Risk Management, Security Training, Plan of Action and Milestone, Remote Access Management, Contingency Planning, and Contractor Systems.

⁸ The Department has not fully implemented corrective actions to ensure only approved or authorized remote access solutions are used; or formally documented procedures for authorizing, monitoring, and controlling all methods of remote access.

This table lists the FISMA reporting metric attributes that a bureau/office has a control deficiency.

Bureau	Program	Recommendation	Deficiencies identified in FY 2015 FISMA Reporting
	Area ⁹	#	Metric Attribute
BLM	CM	Recommendation 1	(NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)
		Recommendations 2 and 3	(b) (7)(E) (NIST SP 800-53: CM-3, SI-2)
	IAM	Recommendation 28	(b) (7)(E)
		Recommendation 29	(b) (7)(E)
	IR	Recommendations 34 and 35	(b) (7)(E) NIST SP 800-53: AU-6, AU-9)
	СР	Recommendations 53 and 54	(b) (7)(E)
BOR	CM	Recommendation 4	(b) (7)(E) (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)
		Recommendation 5	(NIST SP 800-53: CM-3, SI-2)
	IAM	Recommendation 30	(b) (7)(E)
	IR	Recommendations 36 and 37	(b) (7)(E) IST SP 800-53: AU-6, AU-9)
	СР	Recommendation 55	(b) (7)(E) (FCD1, NIST SP 800-34, NIST SP 800-53)

⁹ CMM: Continuous Monitoring Management, CM: Configuration Management, IAM: Identity and Access Management, IR: Incident Response and Reporting, RM: Risk Management, ST: Security Training, POA&M: Plan of Action and Milestones, RAM: Remote Access Management, and CP: Contingency Planning.

BSEE	CM	Recommendations 7 and 8	(NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)
		Recommendation 6	(b) (7)(E) (NIST SP 800-53: CM-3, SI- 2)
FWS	CM	Recommendation 10	(b) (7)(E)
		Recommendation 10	(b) (7)(E)
		Recommendation 9	(NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)
		Recommendation 9	(b) (7)(E) (NIST SP 800-53: CM-3, SI-2)
	IAM	Recommendation 31	(b) (7)(E)
	RM	Recommendation 45	(b) (7)(E)
		Recommendation 44	(b) (7)(E)
	POA&M	Recommendation 50	(b) (7)(E)
	СР	Recommendation 56	(b) (7)(E) (FCD1, NIST SP 800-34, NIST SP 800-53).
NPS	CM	Recommendation 13	(NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)

		Recommendations 11 and 12	(b) (7)(E) (NIST SP 800-53: CM-3, SI-2)
OS/OCIO	CMM	Recommendations	(b) (7)(E)
US/UCIU	CIVIIVI	1 through 59	(b) $(7)(E)$ (b) $(7)(E)$
	CM	Recommendation 16	(b) (7)(E)
		Recommendations 14 and 15	(b) (7)(E) NIST SP 800-53: CM-3, SI- 2)
	IAM	Recommendation 32	(b) (7)(E) (NIST SP 800-53: AC-1).
	IR	Recommendations 40, 41, and 42	(b) (7)(E) (NIST SP 800-53: IR-1).
0.01.07.5		T	
OSMRE	CM	Recommendation 18	(b) (7)(E) (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)
		Recommendation 17	(b) (7)(E) NIST SP 800-53: CM-3, SI- 2)
	IAM	Recommendation 32	(b) (7)(E)
OST	CM	Danaman dation	
OST	CM	Recommendation 20	(b) (7)(E) (NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)
		Recommendation 19	(b) (7)(E) NIST SP 800-53: CM-3, SI- 2)

USGS	CM	Recommendations 21 and 22	(b) (7)(E)	(NIST SP 800-53: CM-4, CM-6, RA-5, SI-2)
		Recommendation 23	(b) (7)(E)	(NIST SP 800-53: CM-3, SI-
	ST	Recommendation 48	(b) (7)(E)	(b) (7)(E)
		Recommendation 49	(b) (7)(E)	(b) (7)(E)
BIA	IAM	Recommendation	(b) (7)(E)	(b) (7)(E)
		27	(b) (7)(E)	
	RM	Recommendation 43		(b) (7)(E)
	ST	Recommendation 47	(b) (7)(E)	(b) (7)(E)
	СР	Recommendation 51	(b) (7)(E)	(b) (7)(E) (NIST SP 800- 34).
		Recommendation 52	(b) (7)(E)	(b) (7)(E)
SOL	CM	Recommendation	(b) (7)(E)	(b) (7)(E)
		26	(b) (7)(E)	
		Recommendation 24	(b) (7)(E)	(b) (7)(E) (NIST SP 800-53: CM-4, CM-6,
		Danes 1.2	(b) (7)(E)	RA-5, SI-2)
		Recommendation 25	52	(b) (7)(E)

			(b) (7)(E) (NIST SP 800-53: CM-3, SI-2)
IAM	Recommendation 33	(b) (7)(E)	(b) (7)(E)
IR	Recommendations 38 and 39	(D) (7)(E	(b) (7)(E) (NIST SP 800-53: AU-6, AU-9)
RM	Recommendation 46	(b) (7)(E)	(b) (7)(E)
CP	Recommendation 58	(b) (7)(E)	(b) (7)(E)
	Recommendations 57 and 58	(b) (7)(E)	(b) (7)(E)
	Recommendation 59	(b) (7)(E)	(b) (7)(E) (FCD1, NIST SP 800-34, NIST SP 800-53).

Appendix II – Listing of Acronyms

Acronym	Definition
A&A	Assessment & Authorizations
AC	Access Control
(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)
ADIR	Associate Director for Information Resources
AO	Authorizing Official
AT	Awareness and Training
ATO	Authority/Authorization to Operate
AU	Audit and Accountability
(b) (7)(E)	(b) (7)(E)
BCISO	Bureau Chief Information Security Officer
ВСР	Business Continuity Plan
BIA	Bureau of Indian Affairs
BLM	Bureau of Land Management
BOR	Bureau of Reclamation
BPA	Business Process Analysis
BSEE	Bureau of Safety and Environmental Enforcement
CA	Security Assessment and Authorization
CIO	Chief Information Officer
CIRC	Computer Incident Response Center
CISO	Chief Information Security Officer
CM	Configuration Management
CMM	Continuous Monitoring
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan

Acronym	Definition
СР	Contingency Planning
CS	Contractor System
(b) (7)(E)	(b) (7)(E)
(b) (7)(E)	(b) (7)(E)
DB	Database
DHS	Department of Homeland Security
DOI	United States Department of the Interior
DRP	Disaster Recovery Plan
EOL	End-of-Life
(b) (7)(E)	(b) (7)(E)
FCD	Federal Continuity Directive
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FISSA+	Federal Information System Security Awareness
(b) (7)(E)	(b) (7)(E)
FWS	US Fish and Wildlife Service
FY	Fiscal Year
(b) (7)(E)	(b) (7)(E)
HQ	Headquarters
HSPD	Homeland Security Presidential Directive
IA	Identification and Authentication
(b) (7)(E)	(b) (7)(E)
IaaS	Infrastructure-as-a-Service
(b) (7)(E)	(b) (7)(E)
IG	Inspector General
0.00	(b) (7)(E)

Acronym	Definition
(b) (7)(E)	(b) (7)(E)
IP	Internet Protocol
IR	Incident Response
ISSO	Information System Security Officer
IT	Information Technology
JAB	Joint Authorization Board
KFM	Key FISMA Metric
KPMG	KPMG LLP
LAN	Local Area Network
(7)(E)	(b) (7)(E)
MOU	Memorandum of Understanding
(b) (7)(E)	(b) (7)(E)
NFR	Notice of Findings and Recommendations
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPS	National Park Service
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
(b) (7)(E)	(b) (7)(E)
OMB	Office of Management and Budget
ONRR	Office of Natural Resources Revenue
OPM	Office of Personnel Management
OS	Office of the Secretary
OS	Operating System
OSMRE	Office of Surface Mining Reclamation and Enforcement
OST	Office of the Special Trustee for American Indians
PII	Personally Identifiable Information

Acronym	Definition
PIN	Personal Identification Number
PIV	Personal Identity Verification
PL	Planning
PM	Program Management
POA&M	Plan of Action and Milestones
PUB	Publication
PY	Prior Year
RA	Risk Assessment
RAM	Remote Access Management
RBST	Role Based Security Training
REV	Revision
RFQ	Request for Quotation
RM	Risk Management
RMF	Risk Management Framework
ROB	Rules of Behavior
SA	System and Services Acquisition
SAN	Storage Area Network
SC	System and Communication Protection
SCAP	Security Content Automation Protocol
SCCM	System Center Configuration Manager
SI	System and Information Integrity
SOL	Office of the Solicitor
SOW	Statement of Work
SP	Special Publication
(b) (7)(E)	(b) (7)(E)
SSP	System Security Plan
ST	Security and Awareness Training

Acronym	Definition
STIG	Security Technical Implementation Guide
(b) (7)(E)	(b) (7)(E)
US	United States
US-CERT	United States Computer Emergency Readiness Team
USGCB	United States Government Configuration Baseline
USGS	United States Geological Survey
(b) (7)(E)	(b) (7)(E)
VM	Virtual Machine
VPN	Virtual Private Network

Appendix III - Prior Year Recommendation Status

Appendix III provides the status of FY2014, FY2013, and FY2012 recommendations; 38 of 56 (68%) remain open. FY2014 recommendation 3 is closed. Below is a summary table of the FY14 FISMA report recommendation and the status.

Table 1. FY2014 FISMA Report Recommendations and Status as of 9/30/2015

	Table 1. FY2014 FISMA Report Recommendations and Status as of 9/30/2015				
	FY2014 FISMA Report Recommendation and Status				
	6 of 7 Recommendations are Open				
ID	Recommendation	OCIO Response as of 9/30/15	Status of 9/30/15 (OPEN or		
			CLOSED		
1	Configuration	FY2012 FISMA Performance Audit	1 OPEN		
	Management: Implement	Recommendation 3 – Implement secure			
	corrective action plans for	baselines for (b) (7)(E)			
	OCIO reference numbers:	[OCIO Ref#: OIG-			
	OIG-0170, Implement	0170] BIA, OCIO, ONRR, OSMRE, OST &			
	secure baselines for	FWS completed corrective actions. OIG &			
	(b) (7)(E)	USGS efforts remain in process. Current			
		target completion date = $1/31/2016$			
	networking	FY2012 FISMA Performance Audit			
	equipment and OIG-0173,	Recommendation 6 – Implement high-risk	2 OPEN		
	Implement high-risk	vulnerabilities and third party vendor security patches in accordance with Department			
	vulnerabilities and third	policy [OCIO Ref #: OIG-0173] BIA, OCIO,			
	party vendor security	NPS & OSMRE completed corrective			
	patches in accordance with	actions. BLM & OIG efforts remain in			
	Department policy.	process. Current target completion date =			
		12/31/2015			
2	Identity and Access	1 FY2012 FISMA Performance Audit	1 OPEN		
	Management: Implement	Recommendation 7 – Implement and document periodic account management			
	corrective action plans for	reviews in accordance with NIST SP-800-53,			
	OCIO reference numbers:	IA-2 and AC-2 [OCIO Ref #: OIG-0174]			
	OIG-0174, Implement and	Closed by PFM on 9/24/2013 based on			
	document periodic account	substantial completion. BLM, NPS, OSMRE,			
	management reviews in	OST & USGS completed corrective actions.			
	accordance with NIST SP-	BIA & OIG efforts remain in process.			
	800-53, IA-2 and AC-2	Current target completion date = 12/31/2015 2 FY2012 FISMA Performance Audit			
	and OIG-0175, Implement	2 FY2012 FISMA Performance Audit Recommendation 8 – Implement and			
	and document	document (b) $(7)(E)$			
	(b) (7)(E)		2 OPEN		
		users in accordance with OMB policy [OCIO			
	users in	Ref#: OIG-0175] [OCIO Ref #: OIG-0175]			
	accordance with OMB	BIA, BOR & OST completed corrective			
	policy.	actions. OCIO must complete & close			
		approve POA&M Id prior to requesting closure with PFM. Current target			
		completion date = 12/31/2015			
3	Identity and Access	[OCIO Ref #: OIG-217] Recommendation should	CLOSED. Recommendation		
	Management: BIA should	read, "BIA should implement a mechanism to	was tested and validated during		
	implement a mechanism to	disable terminated and inactive users accounts	FY15 audit.		
	disable terminated and	after (b) $(7)(E)$. On			
		8/11/2015, PFM email to OIG (K.Elmore) states			
		or 11/2013, FTWI chian to Old (K.Elliole) states			

59

4 Identity and Access Management: BIA should	or Information Resources established and implemented an automated mechanism to remove ind/or deactivate the (b) (7)(E) user accounts." OCIO Ref #: OIG-218] BIA corrective action in rocess. Current target completion date = 2/1/2015	OPEN
5 Risk Management: Implement corrective action plans for OCIO references, OIG-0168, OIG-0179, OIG-0204, and OIG-0171: 1 OIG-0168 - Ensure that all bureaus and offices have documented, approved, and fully implemented a continuous monitoring process in accordance with the DOI Continuous Monitoring Strategic Plan; 2 OIG-0179 - Develop mechanisms to ensure system security plans reflect current operational environments, including complete and accurate controls descriptions and key personnel; 3 OIG-0204 - Ensure bureaus and offices are reviewing POA&Ms and submitting the POA&M Certification Transmittal to the department on a quarterly basis; and 4 OIG-0171- Ensure that each bureau and office	FY2012 FISMA Performance Audit Recommendation 1 [OCIO Ref #: OIG-0168] OST completed corrective actions. BIA, BLM, FWS & OIG efforts remain in process. Current target completion date = 1/15/2016 FY2012 FISMA Performance Audit Recommendation 12 [OCIO Ref #: OIG-0179] OCIO completed corrective actions. BIA, FWS & OIG efforts remain in process. Current target completion date = 12/31/2015 FY2013 FISMA Performance Audit Recommendation 21 [OCIO Ref #: OIG-0204] OIG & OCIO completed corrective actions. BIA & SOL efforts remain in process. Current target completion date = 12/15/2016 FY2012 FISMA Performance Audit Recommendation 4 [OCIO Ref #: OIG-0171] OIG & BIA efforts remain in process. Current target completion date = 3/15/2016	1 OPEN 2 OPEN 3 OPEN 4 OPEN

	with baseline configuration in accordance with Department policy.		
6	Contingency Planning: Implement corrective action plan for OCIO reference number: OIG- 0184 - Ensure information system contingency plans are updated with the required information; plans are fully tested, and lessons learned are communicated to senior management.	FY2012 FISMA Performance Audit Recommendation 17 [OCIO Ref #: OIG-0184] OIG completed corrective actions. BIA efforts remain in process. Current target completion date = 1/15/2016	OPEN
7	Security Awareness and Training: Implement corrective action plan for OCIO reference number: OIG-0181- Implement a mechanism to ensure all employees and contractors complete required security awareness training; and ensure personnel with specialized security responsibilities fulfill annual specialized computer security training requirements.	FY2012 FISMA Performance Audit Recommendation 14 [OCIO Ref #: OIG-0181] OCIO completed corrective actions. BIA & FWS efforts remain in process. Current target completion date = 7/31/2016	OPEN

FY2013 recommendations 5, 9, 11, 12, 13, 15, 16, 22, 25, 26 and 29 are closed. Management considers FY2013 recommendation 23 and 24. We disagree and consider the recommendations open until correctives actions are fully implemented and tested to determine operating effectiveness. Below is a summary table of the FY13 FISMA report recommendation and the status.

Table 2. FY2013 FISMA Report Recommendations and status as of 9/30/2015.

	Table 2. FY2013 FISMA Report Recommendations and status as of 9/30/2015.			
	FY2013 FISMA Report Recommendation and Status 18 of 29 Recommendations are Open			
	ID Recommendation OCIO Response as of 9/30/15 Status as of 9/30/15			
ш	Recommendation	OCIO Response as of 9/30/15	(OPEN or CLOSED)	
1	Continuous	FY2012 FISMA Performance Audit Recommendation 1	OPEN	
	Monitoring	[OCIO Ref #: OIG-0168] OST completed corrective		
	Management: Ensure	actions. BIA, BLM, FWS & OIG efforts remain in		
	that all bureaus and	process. Current target completion date = 1/15/2016		
	offices have	T		
	documented,			
	approved, and fully			
	implemented a			
	continuous			
	monitoring process			
	in accordance with			
	the DOI Office of			
	the Chief			
	Information Officer			
	(OCIO)			
	Memorandum,			
	Ongoing Assessment			
	and Authorization			
	Through Continuous			
	Monitoring, dated			
	March 16, 2012 and			
	OCIO Directive			
	2010-009.			
2	Continuous	FY2012 FISMA Performance Audit Recommendation 1	OPEN	
	Monitoring	[OCIO Ref #: OIG-0168] OST completed corrective		
	Management:	actions. BIA, BLM, FWS & OIG efforts remain in		
	Implement a process	process. Current target completion date = 1/15/2016		
	to ensure bureaus			
	and offices have			
	completed security			
	control evaluations over information			
	systems in accordance with			
	their respective			
	continuous			
	monitoring plans.			
3	Configuration	[OCIO Ref#: OIG-0195] BSEE, OCIO & OIG completed	OPEN	
	Management:	corrective actions. BLM, BOR, FWS & SOL completion	51 L11	
	Ensure that DOI	efforts remain in process. Current target completion date		
	management reviews	= 12/31/2015		
	management reviews	IBIGIIBUIG	I	

			,
	and updates		
	configuration		
	management		
	procedures on at		
	least an (b) $(7)(E)$.		
4	Configuration	FY2012 FISMA Performance Audit Recommendation 6	OPEN
	Management:	[OCIO Ref #: OIG-0173] BIA, OCIO, NPS & OSMRE	
	Remediate high-risk	completed corrective actions. BLM & OIG efforts remain	
	vulnerabilities and	in process. Current target completion date = 12/31/2015	
	implement third		
	party vendor (b) (7)(E)		
	(b) (7)(E) in		
	accordance with		
	Department policy.		
6	Configuration	FY2012 FISMA Performance Audit Recommendation 4	OPEN
	Management: Ensure	[OCIO Ref #: OIG-0171] BIA & OIG efforts remain in	
	that each bureau and	process. Current target completion date = 3/15/2016	
	office assesses		
	compliance with		
	baseline		
	configurations in accordance with		
	Department policy.		
7	Configuration	FY2012 FISMA Performance Audit Recommendation 7	OPEN
	Management:	[OCIO Ref #: OIG-0174] Closed by PFM on 9/24/2013	
	Implement standard	based on substantial completion. BLM, NPS, OSMRE,	
	baselines such as	OST & USGS completed corrective actions. BIA & OIG	
	(b) $(7)(E)$	efforts remain in process. Current target completion date	
		= 12/31/2015	
8	Configuration	[OCIO Ref #: OIG-0196] As of 8/10/2015, BLM efforts	OPEN
	Management: Ensure	remain in process. Current Target Completion Date =	
	unsupported	10/30/2015	
	Operating Systems		
	are not used in		
	production		
10	environments.	[OCIO Pof#, OIC 0107] PREE NIBS & OIC11	OPEN
10	Identity and Access Management:	[OCIO Ref #: OIG-0197] BSEE, NPS & OIG completed corrective actions. BLM, BOR, & SOL efforts remain in	OPEN
	Ensure bureaus and	process. Current target completion date = 12/31/2015.	
	offices completely	process. Current target completion date = 12/31/2013.	
	document procedures		
	for account and		
	identity management		
	in accordance with		
	Departmental		
	Security Control		
	Standards for Access		

	Control and		
	Identification and		
	Authentication.		
13	Incident Response and Reporting: Ensure the OIG has reviewed or updated incident and response reporting on an annual basis.	Recommendation validated during the FY2015 FISMA audit.	CLOSED
14	Risk Management: Ensure bureaus and offices have completely documented procedures in accordance with the DOI IT Security Control Standards.	[OCIO Ref#: OIG-0200] BSEE, NPS & OIG completed corrective actions. SOL efforts remain in process. Current target completion date = 12/31/2015.	OPEN
17	Risk Management: Ensure bureaus and offices maintain an up-to-date information system inventory for completeness and accuracy.	FY2010 FISMA Performance Audit Recommendation 3 [OIG-0019]. Corrective actions continuing. Current target completion date = 2/28/2016	OPEN
18	Risk Management: Ensure SOL maintains security authorization and assessment documentation in (5) (7)(E) in accordance with the Department Plan of Action and Milestone Process Standard.	[OCIO Ref#: OIG-0201] SOL completion of planned corrective actions continuing.	OPEN
19	Security Training: Ensure OIG personnel complete required Federal Information System Security Awareness Training in accordance with departmental security awareness policy.	[OCIO Ref#: OIG-0202] OIG corrective actions completed, management awaiting formal notification.	OPEN
	poncy.	64	<u> </u>

20	Security Training:	[OCIO Ref #: OIG-0203] BLM & OIG corrective actions	OPEN
	BLM and OIG	completed, management awaiting formal notication.	
	review and update	1 , 5	
	security awareness		
	training procedures		
	on at least an annual		
	basis in accordance		
	with policy.		
21	Plan of Action and	[OCIO Ref #: OIG-0204] OIG & OCIO corrective	OPEN
	Milestones:	actions completed. BIA & SOL efforts continuing.	
	Ensure bureaus and	Current target completion date = 12/15/2016	
	offices are reviewing		
	POA&Ms and		
	submitting the		
	POA&M		
	Certification		
	Transmittal to the		
	department on a		
	quarterly basis.		
23	Remote Access	FY2012 FISMA Performance Audit Recommendation 16	OPEN. Although management
	Management:	[OCIO Ref #: OIG-0183] On 10/2/2014, Memo from Eric	considers this recommendation
	Ensure BLM, BSEE,	Eisenstein (PFM) [signed by Nancy Thomas] to	closed, KPMG disagrees
	and OIG are utilizing	Kimberly Elmore (AIG) states in part, "The [OCIO] has	because DOI has not fully
	an approved or	asserted that it has taken the actions necessary to	implemented corrective actions
	authorized solution	implement Recommendation 16, in the subject audit	and tested operating
	for remote access.	report Upon reviewing the attached supporting	effectiveness.
		documentation, PFM determined that the OCIO has met	
		the intent of the recommendation and considers the	
		recommendation implemented."	
24	Remote Access	2012 FISMA Performance Audit Recommendation 16	OPEN. Although management
	Management:	[OCIO Ref #: OIG-0183] On 10/2/2014, Memo from Eric	considers this recommendation
	Implement a process	Eisenstein (PFM) [signed by Nancy Thomas] to	closed, KPMG disagrees
	to ensure bureaus	Kimberly Elmore (AIG) states in part, "The [OCIO] has	because DOI has not fully
	and offices have	asserted that it has taken the actions necessary to	implemented corrective actions
	formally documented	implement Recommendation 16, in the subject audit	and tested operating
	procedures for	report Upon reviewing the attached supporting	effectiveness.
	authorizing,	documentation, PFM determined that the OCIO has met	
	monitoring, and	the intent of the recommendation and considers the	
	controlling all	recommendation implemented."	
	methods of remote		
	access.		
27	Contingency	FY2012 FISMA Performance Audit Recommendation 17	OPEN
	Planning:	[OCIO Ref #: OIG-0184] BIA & OIG efforts remain in	
	Enhance the	process. Current target completion date = $1/15/2016$	
	contingency		
	planning process to		
	include analysis of		
	information system		
	business impact		
	analysis into the		

	continuity of operations plan.		
28	Contingency Planning: Ensure contingency plan tests and exercises are conducted in accordance with NIST SP 800-53 requirements.	FY2012 FISMA Performance Audit Recommendation 17 [OCIO Ref #: OIG-0184] BIA & OIG efforts remain in process. Current target completion date = 1/15/2016	OPEN

FY2012 recommendations 5, 11, 13, 15, 19, and 20 are closed. Below is a summary table of the FY 12 FISMA report recommendation and the status.

Table 3. FY2012 FISMA Report Recommendations and status as of 9/30/2015.

	FY2012 FISMA Report Recommendation and Status FY2012 FISMA Report Recommendation and Status			
	14 of 20 Recommendations are Open			
ID	Recommendation	OCIO Response as of 9/30/15	Status as of 9/30/15 (OPEN or CLOSED)	
1	Continuous Monitoring Management: Ens ure that all bureaus and offices have documented, approved, and fully implemented a continuous monitoring process in accordance with the DOI Continuous Monitoring Strategic Plan.	[OCIO Ref #: OIG-0168] OST corrective actions completed. BIA, BLM, FWS & OIG efforts remain in process. Current target completion date = 1/15/2016	OPEN	
2	Configuration Management: Impl ement Security Technical Implementation Guide (STIG) when available and document exceptions to secure baseline.	[OCIO Ref #: OIG-0169] OCIO, ONRR, OST & USGS corrective actions completed. BIA & OIG efforts remain in process. Current target completion date = 12/31/2015	OPEN	
3	Configuration Management: Implement secure baselines for (b) (7)(E)	[OCIO Ref #: OIG-0170] BIA, OCIO, ONRR, OSMRE, OST & FWS corrective actions completed. USGS efforts in process. Current target completion date = 1/31/2016	OPEN	
4	Configuration Management: Ens ure that each bureau and office assesses compliance with baseline	[OCIO Ref #: OIG-0171] OIG & BIA efforts continuing. Current target completion date = 3/15/2016	OPEN	

	configuration		
	in accordance with		
	Department policy.		ODEN
6	Configuration	[OCIO Ref#: OIG-0173] BIA, OCIO, NPS & OSMRE	OPEN
	Management: Impl	corrective action completed. BLM & OIG efforts	
	ement high-risk	continuing. Current target completion date = 12/31/2015	
	vulnerabilities and		
	third party vendor		
	security patches in		
	accordance with		
	Department policy.		
7	Identity & Access	[OCIO Ref#: OIG-0174] Closed by PFM on 9/24/2013	OPEN
	Management: Impl	based on substantial completion. BLM, NPS, OSMRE,	
	ement and	OST & USGS corrective action completed. BIA & OIG	
	document periodic	efforts continuing. Current target completion date =	
	account	12/31/2015	
	management		
	reviews in		
	accordance with		
	NIST SP-800-53,		
	IA-2 and AC-2.		
8	Identity & Access	[OCIO Ref #: OIG-0175] BIA, BOR & OST corrective	OPEN
	Management: OCI	action completed. OCIO efforts to complete & close	
	O: Implement and	POA&M Id 27404 continuing. Current target completion	
	document PIV	date = 12/31/2015	
	smartcard usage for		
	logical access for		
	privileged and non-		
	privileged users in		
	accordance with		
	OMB policy.		
9	Incident	[OCIO Ref #: OIG-0176] OCIO closure request sent on	OPEN
	Response: Ensure	behalf of OIG to PFM on 9/22/2015 and confirmed as	
	OIG updates	completed on 9/25/2015.	
	incident response		
	and reporting		
	procedures in		
	accordance with		
	NIST SP 800-61.		
10	Incident	[OCIO Ref #: OIG-0177] OIG efforts continuing. Current	OPEN
	Response: Implem	target completion date is 12/31/2015	
	ent a security event		
	and incident		
	correlation		
	solution, to monitor		
	security for all		
	systems,		
	interconnections,		
	and network		
	segments		
	supporting the OIG		

	bureau and		
	operations.		
11	Incident	Recommendation tested and validated during the FY2015	CLOSED
	Response: Implem	FISMA audit.	Recommendation validated
	ent a process and		during the FY2015 FISMA
	mechanism to		audit.
	monitor and report		
	on incident		
	response timelines		
	and assess bureau		
	adherence to those		
	timelines.		
12	Risk Management:	[OCIO Ref #: OIG-0179] OCIO corrective actions	OPEN
	Develop	completed. BIA, FWS & OIG efforts remain in process.	
	mechanisms to	Current target completion date = 12/31/2015	
	ensure system		
	security plans		
	reflect current		
	operational		
	environments,		
	including complete		
	and accurate		
	controls		
	descriptions and		
	key personnel.		
13	Risk	[OCIO Ref #: OIG-0180] Closed by PFM on 9/25/2014	CLOSED
	Management: Mai	based on substantial completion. BOR & ONRR	Recommendation validated
	ntain security	completed corrective actions prior to 9/25/2014 & BLM	during the FY2015 FISMA
	authorization	completed on 10/16/2014. Corrective actions completed.	audit.
	documentation in		
	(b) (7)(E) in		
	accordance with		
	the Department of		
	Justice (b) (7)(E)		
	Users Guide, dated		
	(b) (7)(E)		
14	Security	[OCIO Ref #: OIG-0181] OCIO completed corrective	OPEN
	Training: Impleme	actions. BIA & FWS efforts continuing. Current target	
	nt a mechanism to	completion date = $7/31/2016$	
	ensure all		
	employees and		
	contractors		
	complete required		
	security awareness		
	training; and ensure		
	personnel with		
	specialized security		
	responsibilities		
	fulfill annual		
	specialized		
	computer security		

	training		
	requirements.		
16	Remote	[OCIO Ref #: OIG-0183] On 10/2/2014, Memo from Eric	OPEN. Although management
10	Access: OCIO: C	Eisenstein (PFM) [signed by Nancy Thomas] to Kimberly	considers this recommendation
	omplete the	Elmore (AIG) states in part, "The [OCIO] has asserted that	closed, KPMG disagrees
	implementation of	it has taken the actions necessary to implement	because DOI has not fully
	OCIO Directive	Recommendation 16, in the subject audit report Upon	implemented corrective actions
	2012-008. Take	reviewing the attached supporting documentation, PFM	and tested operating
	action to enforce	determined that the OCIO has met the intent of the	effectiveness.
	two -factor	recommendation and considers the recommendation	chectiveness.
	authentication,	implemented."	
	prohibit single-	implemented.	
	factor remote		
	access except for		
	temporary		
	exceptions, and		
	ensure the		
	allowable		
	exceptions are		
	uniformly defined		
	and enforced across		
	all bureaus and		
	offices.		
17	Contingency	[OCIO Ref #: OIG-0184] OIG corrective actions	OPEN
1,	Planning: Ensure	completed. BIA efforts continuing. Current target	OT ET
	information system	completion date = $1/15/2016$	
	contingency plans	1713/2010	
	are updated with		
	the required		
	information; plans		
	are fully tested, and		
	lessons learned are		
	communicated to		
	senior		
	management.		
18	Contingency	[OCIO Ref #: OIG-0185] Closed by PFM on 5/9/2013	OPEN
	Planning:	based on substantial completion. OCIO & USGS	
	Ensure the	corrective action completed. BLM, FWS & OIG efforts	
	Department, to	continuing. Current target completion date = 12/31/2015	
	include Bureaus		
	and Offices,		
	conduct business		
	impact analysis to		
	identify impact of		
	any unplanned		
	disruption of		
	critical information		
	processing systems		
	or other key assets,		
	identify sources of		
	threats and		

vulnerabilities	
which could lead to	
unplanned outages	
or disruption of	
service, and	
implement	
safeguards to	
minimize the	
likelihood should	
any identified	
threats occur.	

Appendix IV – NIST SP 800-53 Security Controls Cross-Referenced to FY2015 OIG FISMA Metrics

The table below represents NIST SP 800-53 security controls that KPMG considered during the performance audit.

Continuous Monitorius Monas annut		
Continuous Monitoring Management		
CA-1	Security Assessment and Authorization Policies and Procedures	
CA-2	Security Assessments	
CA-5	Plan of Action and Milestones	
CA-7	Continuous Monitoring	
	ation Management	
CM-1	Configuration Management Policy and Procedures	
CM-2	Baseline Configurations	
CM-3	Configuration Change Control	
CM-4	Security Impact Analysis	
CM-6	Configuration Settings	
CM-7	Least Functionality	
CM-8	Information System Component Inventory	
RA-5	Vulnerability Scanning	
SI-2	Flaw Remediation	
Identity a	nd Access Management	
AC-1	Access Control Policy and Procedures	
AC-2	Account Management	
AC-10	Concurrent Session Control	
AC-11	Session Lock	
AC-17	Remote Access	
AC-18	Wireless Access	
IA-2	Identification and Authentication	
IA-3	Device Identification and Authentication	
Incident a	and Response Reporting	
IR-1	Incident Response Policy and Procedures	
IR-4	Incident Handling	
IR-5	Incident Monitoring	
IR-6	Incident Reporting	
IR-7	Incident Response Assistance	
IR-8	Incident Response Plan	
AU-6	Audit Review, Analysis, and Reporting	
AU-9	Protection of Audit Information	
Risk Mar	nagement	
RA-1	Risk Assessment Policy and Procedures	
RA-2	Security Categorization	
CA-2	Security Assessments	
CA-6	Security Authorization	
CA-7	Continuous Monitoring	
PL-2	System Security Plan	
PM-5	Information System Inventory	
SI-3	Malicious Code Protection	
SI-4	Information System Monitoring	
SI-8	Spam Protection	
AU-2	Auditable Events	

AU-3	Content of Audit Records
Security 7	Training
AT-1	Security Awareness and Training Policy and Procedures
AT-3	Security Training
AT-4	Security Training Records
Plan of A	ction and Milestone
CA-5	Plan of Action and Milestones
PM-3	Information Security Resources
PM-4	Plan of Action and Milestones Process
Remote A	Access Management
AC-1	Access Control Policy and Procedures
AC-17	Remote Access
PL-4	Rules of Behavior
PS-6	Access Agreements
IA-2	Identification and Authentication
IR-6	Incident Reporting
	ncy Planning
CP-1	Contingency Planning Policy and Procedures
CP-2	Contingency Plan
CP-4	Contingency Plan Testing and Exercises
CP-7	Alternate Processing Site
CP-9	Information System Backup
SA-12	Supply Chain Protection
Contractor Systems	
CA-2	Security Assessments
PL-2	System Security Plan
PM-5	Information System Inventory
SA-1	System and Services Acquisition Policy and Procedures
SA-4	Acquisitions

Appendix V – 2015 FISMA Reporting Metrics

The following tables contain our responses to the control metrics established by DHS for the annual OIG FISMA Reporting Metrics.

In addition, the FY2015 metrics highlight White House Administration FISMA cyber security priorities, which are based on Federal government mandates and the most cost-effective Federal-wide security controls the Department can use to enhance the security of information systems.

Each question, except for question number 1, can have one of two possible responses. Response "Yes" indicates, "The Agency has established and is maintaining a program [for that control metric] that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines." Response "No" indicates, "The Agency has not established a program [for that control metric].

For the continuous monitoring management section below, the response could be either Level 1 Ad-hoc, Level 2 Defined, Level 3 Consistently Implemented, Level 4 Managed and Measureable, or Level 5 Optimized.

Response	
Yes	No control deficiencies noted
No	Control deficiencies were identified

1.	Information Security Continuous Monitoring Management	Response
	Questions	Maturity Level ¹⁰
	1.1. Utilizing the attributes outlined in Appendix VI, please assess the maturity of the organization's program along the domains of people, processes, and technology. Provide a maturity level for each of these domains as well as for the program overall.	People Domain: Level 2 - Defined Technology Domain: Level 1 - Ad-Hoc Process Domain: Level 1 - Ad-Hoc Overall Maturity Level: 1 - Ad-Hoc
	1.2. Please provide any additional information on the effectiveness of the Organization's (b) (7)(E) Program that was not noted in the maturity model above.	
	Explanation: People domain: Level two Defined. The Department has defined responsibilities for stakeholders; however, stakeholders may not have adequate resources (people, processes, and technology) to effectively implement activities. Process domain: Level one Ad-hoc. The Department has not identified and defined the qualitative and quantitative performance measures that will be used to assess the	

¹⁰ To reach a particular level of maturity, DOI should meet all of the attributes outlined in Appendix VI for that respective level. For instance, to reach a Level 2 for the people domain, DOI should meet attributes 1.2.1 to 1.2.4. Similarly, to reach Level 2 for the program overall, DOI should meet attributes 1.2.1 to 1.2.10. When determining the overall maturity level, the lowest common denominator approach applies. For instance, if DOI is at Level 1 for the people domain but at Level 3 for both the processes and technology domains, the overall maturity of DOI's (b) (7)(E) program would be Level 1. 74

1.	Information Security Continuous Monitoring Management	Response
	Questions	Maturity Level ¹⁰
	effectiveness of its ontrol program, achieve situational awareness, and control ongoing risk. Also, the Department has not defined its processes for collecting and considering lessons learned to improve processes. Technology domain: Level one Ad-hoc. The Department has not identified and defined the processes needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. The Department program focuses on four security automation controls areas such as vulnerability management, patch management, asset management and configuration management; however, the use of technologies in the following areas are not fully defined, license management, information management, software assurance, event management, network management, malware detection and incident management. In addition, the Department has not defined how it will use automation to produce an accurate point-in-time inventory of the authorized and unauthorized devices and software on its network. The Department leverages the implementation of a multi-phased Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) initiatives to enhance the overall DOI program.	

2.	Configuration Management	Response
	Questions	Yes/No
	2.1. Has the organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No
	Configuration management control deficiencies were noted at 10 of 13 bureaus and offices, Bureau of Land Management (BLM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE), U.S. Fish and Wildlife Service (FWS), National Park Service (NPS), Office of the Chief Information Officer (OCIO), Office of Surface Mining (OSMRE), Office of the Special Trustee for American Indians (OST), U.S. Geological Survey (USGS), and the Office of the Solicitor (SOL).	
	2.2. Please provide any additional information on the effectiveness of the Organization's Configuration Management Program that was not noted in the questions above.	
	2.3 Does the organization have an enterprise deviation handling process and is it integrated with the automated scanning capability?	Yes
	Explanation:	

3.	Identity and Access Management	Response
	Questions	Yes/No
	3.1. Has the organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices?	No
	3.2. Please provide any additional information on the effectiveness of the Organization's Identity and Access Management Program that was not noted in the questions above.	
	Explanation: Identity and access management control deficiencies were noted at 8 of 13 bureaus and offices, BIA, BLM, BOR, FWS, NPS, OCIO, OSMRE, and SOL.	

4.	Incident Response and Reporting	Response
	Questions	Yes/No
	4.1. Has the organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No
	4.2. Please provide any additional information on the effectiveness of the Organization's Incident Management Program that was not noted in the questions above. Four of 13 bureaus and offices, BLM, BOR, OSMRE, and SOL do not effectively review system audit logs for inappropriate or suspicious activity.	
	Explanation: Incident Response and Reporting management control deficiencies were noted at 5 of 13 bureaus and offices, BLM, BOR, OCIO, OSMRE, and SOL.	

5.	Risk Management	Response
	Questions	Yes/No
	5.1. Has the organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No
	5.2. Please provide any additional information on the effectiveness of the Organization's Risk Management Program that was not noted in the questions above.	
	Explanation: Risk management control deficiencies were noted for 3 of 13 bureaus and offices, BIA, FWS, and SOL.	

5.	Risk Management	Response
	Questions	Yes/No

6.	Security Training	Response
	Questions	Yes/No
	6.1. Has the organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No
	6.2. Please provide any additional information on the effectiveness of the Organization's Security Training Program that was not noted in the questions above.	
	Explanation: Security Training control deficiencies were noted at 2 of 13 bureaus and offices, BIA and USGS.	

7.	Plan of Action and Milestones (POA&M)	Response
	Questions	Yes/No
	7.1. Has the organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses?	No
	7.2. Please provide any additional information on the effectiveness of the Organization's POA&M Program that was not noted in the questions above.	
	Explanation: Plan of action and milestones (POA&M) control weaknesses were noted at one of 13 bureaus and offices, FWS.	

8.	Remote Access Management	Response
	Questions	Yes/No
	8.1. Has the organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No
	8.2. Please provide any additional information on the effectiveness of the organization's Remote Access Management that was not noted in the questions above.	
	8.3. Does the organization have a policy to detect and remove unauthorized (rogue) connections?	No
	Explanation: Prior year deficiencies in this area continue to exist.	

9.	Contingency Planning	Response
	Questions	Yes/No
	9.1. Has the organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines?	No
	9.2. Please provide any additional information on the effectiveness of the organization's Contingency Planning Program that was not noted in the questions above.	
	Explanation: Contingency plan program control deficiencies were noted at 5 of 13 bureaus and offices, BIA, BLM, BOR, FWS, and SOL.	

10.	Contractor Systems	Response
	Questions	Yes/No
	10.1. Has the organization established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to the organization?	No
	10.2. Please provide any additional information on the effectiveness of the organization's Contractor Systems Program that was not noted in the questions above.	
	Explanation: A control deficiency was noted at one bureau and office, OCIO.	

Year 2015. Source: Council of the Inspector General for Integrity and Efficiency (CIGIE)

The purpose of the maturity model is to (1) summarize the status of agencies' information security programs and their maturity on a 5-level scale, (2) provide transparency to agency CIOs, top management officials, and other interested readers of OIG FISMA reports about what has been accomplished and what still needs to be implemented to improve the information security program to the next maturity level, and (3) help ensure consistency across the OIGs in their annual FISMA reviews.

Program Maturity Level	Definition	People	Processes	Technology
Level 1	1.1 (b) (7)(E)	1.1.1 (b) (7)(E) stakeholders and	1.1.5 (b) (7)(E) processes have not	1.1.9 The organization has not
	program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO	their responsibilities have not been fully defined and communicated across the organization. 1.1.2 The organization has not performed an assessment of the skills, knowledge, and resources needed to effectively implement an official program. Key personnel do not possess knowledge, skills, and abilities to successfully implement an effective program. 1.1.3 The organization has not defined how information will be shared with individuals with significant security responsibilities and used to make risk-based decisions. 1.1.4 The organization has not defined how it will integrate of the integration of the integrate of the integration of the integr	1.1.5 Drope processes have not been fully defined and are performed in an ad-hoc, reactive manner for the following areas: ongoing assessments and monitoring of security controls; performing hardware asset management, software asset management, configuration setting management, and common vulnerability management; collecting security related information required for metrics, assessments, and reporting; analyzing of the appropriate risk responses; and reviewing and updating the appropriate risk responses; and reviewing and updating the program. 1.1.6 The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its organizational awareness, and control ongoing risk.	1.1.9 The organization has not identified and defined the technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective. Use of technologies in the following areas is ad-hoc. -Patch management -License management -License management -Software assurance -Vulnerability management -Event management -Malware detection -Asset management -Network management -Incident manag
		requirements.	1.1.8 The organization has not defined its processes for collecting and considering lessons learned to improve processes.	

Program Maturity	Definition	People	Processes	Technology
Level				
Level 2	2.1 The	2.1.1 (b) (7)(E) stakeholders	2.1.5 (b) (7)(E) processes have been	2.1.9 The organization has
Defined	organization	and their responsibilities	fully defined for the following areas:	identified and fully defined the
	has formalized	have been defined and	ongoing assessments and monitoring	(b) (7)(E) technologies it plans to
	its (b) (7)(E)	communicated across the	of security controls; performing	utilize in the following
	program	organization. However,	hardware asset management, software	automation areas. In addition,
	through the	stakeholders may not have	asset management, configuration	the organization has developed
	development	adequate resources (people,	setting management, and common	a plan for implementing (b) (7)(E)
	of	processes, and technology)	vulnerability management; collecting	technologies in these areas:
	comprehensive	to effectively implement	security related information required	patch management, license
	(b) (7)(E)	activities.	for metrics, assessments, and	management, information
	policies,	2.1.2.77	reporting; analyzing (b) (7)(E) data,	management, software
	procedures,	2.1.2 The organization has performed an assessment of	reporting findings, and determining	assurance, vulnerability
	and strategies consistent with	the skills, knowledge, and	the appropriate risk responses; and reviewing and updating the	management, event management, malware
	NIST SP 800-	resources needed to	program. However, these processes	detection, asset management,
	53, SP 800-	effectively implement an	are inconsistently implemented across	configuration management,
	137, OMB M-	(b) (7)(E) program. In	the organization.	network management, and
	14-03, and the	addition, the organization	are organization.	incident management.
	CIO ISCM	has developed a plan for	2.1.6 (b) (7)(E) results vary depending on	However, the organization has
	CONOPS.	closing any gaps identified.	who performs the activity, when it is	not fully implemented
	However,	However, key personnel	performed, and the methods and tools	technology is these automation
	(b) (7)(E)	may still lack the	used.	areas and continues to rely on
	policies,	knowledge, skills, and		manual/procedural methods in
	procedures,	abilities to successfully	2.1.7 The organization has identified	instances where automation
	and strategies	implement an effective	and defined the performance measures	would be more effective. In
	are not	(b) (7)(E) program.	and requirements that will be used to	addition, while automated tools
	consistently		assess the effectiveness of its (b) (7)(E)	are implemented to support
	implemented	2.1.3 The organization has	program, achieve situational	some (b) (7)(E) activities, the tools
	organization-	defined how (b) (7)(E)	awareness, and control ongoing risk.	may not be interoperable.
	wide.	information will be shared	However, these measures are not	
		with individuals with	consistently collected, analyzed, and	2.1.10 The organization has
		significant security	used across the organization.	defined how it will use
		responsibilities and used to	04077	automation to produce an
		make risk-based decisions.	2.1.8 The organization has a defined	accurate point-in-time
		However, b)(7)(E) information is not always	process for capturing lessons learned on the effectiveness of its	inventory of the authorized and unauthorized devices and
		shared with individuals	program and making necessary	software on its network and the
		with significant security	improvements. However, lessons	security configuration of these
		responsibilities in a timely	learned are not consistently shared	devices and software.
		manner with which to	across the organization and used to	However, the organization
		make risk-based decisions.	make timely improvements to the	does not consistently
			(b) (7)(E) program.	implement the technologies
		2.1.4 The organization has	1 5	that will enable it to manage an
		defined how it will		accurate point-in-time
		integrate (b) (7)(E) activities		inventory of the authorized and
		with organizational risk		unauthorized devices and
		tolerance, the threat		software on its network and the

environment, and security config	uration of these
business/mission requirements. However, toological activities are not consistently integrated with the organization's risk management program.	

(b) (7)(E) Program Maturity Level	Definition	People	Processes	Technology
Level 3	3.1 In	3.1.1 (b) (7)(E) stakeholders	3.1.5 (b) (7)(E) processes are consistently	3.1.9 The organization has
Consistent	addition to	and their responsibilities	performed across the organization in	consistently implemented its
ly	the	have been identified and	the following areas: ongoing	defined technologies in all of
Implement	formalizatio	communicated across the	assessments and monitoring of security	the following (b) (7)(E)
ed	n and	organization, and	controls; performing hardware asset	automation areas. (b) (7)(E) tools
	definition of	stakeholders have adequate	management, software asset	are interoperable to the extent
	its (b) (7)(E)	resources (people,	management, configuration setting	practicable.
	program	processes, and technology)	management, and common	
	(Level 2),	to effectively implement	vulnerability management; collecting	-Patch management
	the	(b) (7)(E) activities.	security related information required	-License management
	organization		for metrics, assessments, and	-Information management
	consistently	3.1.2 The organization has	reporting; analyzing (b) (7)(E) data,	-Software assurance
	implements	fully implemented its plans	reporting findings, and determining the	-Vulnerability management
	its (b) (7)(E)	to close any gapes in skills,	appropriate risk responses; and	-Event management
	program	knowledge, and resources	reviewing and updating the (b)(7)(E)	-Malware detection
	across the	required to successfully	program.	-Asset management
	agency.	implement ar (b) (7)(E)		-Configuration management
	However,	program. Personnel possess	3.1.6 The rigor, intensity, scope, and	-Network management
	qualitative	the required knowledge,	results of activities are	-Incident management
	and	skills, and abilities to	comparable and predictable across the	
	quantitative	effectively implement the	organization.	3.1.10 The organization can
	measures	organization's (b) (7)(E)		produce an accurate point-in-
	and data on	program.	3.1.7 The organization is consistently	time inventory of the
	the	a da (INVIVEL) da di di	capturing qualitative and quantitative	authorized and unauthorized
	effectiveness	3.1.3 information is	performance measures on the	devices and software on its
	of the (b) (7)(E)	shared with individuals	performance of its (0) (7)(=) program in	network and the security
	program	with significant security		configuration of these devices and software.
	across the	responsibilities in a	requirements for data collection, storage, analysis, retrieval, and	and software.
	organization are not	consistent and timely manner with which to make	reporting. (b)(7)(E) measures provide	
	captured and	risk-based decisions and	information on the effectiveness of	
	utilized to	support ongoing system	processes and activities.	
	make risk-	authorizations.	processes and activities.	
	based	GGAIOILAGOIS.	3.1.8 The organization is consistently	
	decisions,	3.1.4 (b) (7)(E) activities are	capturing and sharing lessons learned	
	consistent	fully integrated with	on the effectiveness of (5) (7)(E)	
	with NIST	organizational risk	processes and activities. Lessons	
	SP 800-53,	tolerance, the threat	learned serve as a key input to making	
	SP 800-137,	environment, and	regular updates to (b) (7)(E) processes.	
	OMB M-14-	business/mission		
	03, and the	requirements.		
	CIO ISCM	_		
	CONOPS.			

Program Maturity Level	Definition	People	Processes	Technology
Level 4 Managed	4.1 In addition to	_		_
Maturity Level	4.1 In	4.1.1 The organization's staff is consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of the organization's program. 4.1.2 Skilled personnel have been hired and/or existing staff trained to develop the appropriate metrics to measure the success of the program. 4.1.3 Staff are assigned responsibilities for developing and monitoring metrics, as well as updating and revising metrics as needed based on organization risk tolerance, the threat environment, business/mission requirements, and the results of the program.	4.1.4 The organization has processes for consistently implementing, monitoring, and analyzing qualitative and quantitative performance measures across the organization and is collecting, analyzing, and reporting data on the effectiveness of its processes for performing (at the consistent of the processes for performing (at the processes for performance measures across the performance measures across (at the performance measures across (at the performance measures across (at the performing (at the performance performing (at the performance performing (at the performance performing (at the performing (at the performance performing (at the performing (at the performing (at the performing (at the performance performing (at the pe	4.1.10 The organization uses technologies for consistently implementing, monitoring, and analyzing qualitative and quantitative performance across the organization and is collecting, analyzing, and reporting data on the effectiveness of its technologies for performing (a) (a) (b) (c) (c) (c) (d) (e) (e) (e) (e) (e) (e) (e) (e) (e) (e
			ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required	
			system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis.	

(b)(7)(E) Program Maturity Level	Definition	People	Processes	Technology
Level 5	5.1 In	5.1.1 The organization's	5.1.2 The organization has	5.1.6 The organization has
Optimized	addition to	assigned personnel	institutionalized a process of	institutionalized the
	being	collectively possess a high	continuous improvement incorporating	implementation of advanced
	managed	skill level to perform and	advanced cybersecurity and practices.	cybersecurity technologies in
	and	update (b) (7)(E) activities on a		near real-time.
	measurable	near real-time basis to make	5.1.3 On a near real-time basis, the	
	(Level 4),	any changes needed to	organization actively adapts its 1 organization	5.1.7 The organization has
	the	address (b) (7)(E) results based	program to a changing cybersecurity	institutionalized the use of
	organization	on organization risk	landscape and responds to evolving	advanced technologies for
	's (b) (7)(E)	tolerance, the threat	and sophisticated threats in a timely	analysis of trends and
	program is	environment, and	manner.	performance against
	institutional	business/mission		benchmarks to continuously
	ized,	requirements.	5.1.4 The (b) (7)(E) program is fully	improve its (b) (7)(E) program.
	repeatable,		integrated with strategic planning,	
	self-		enterprise architecture and capital	
	regenerating		planning and investment control	
	, and		processes, and other mission/business	
	updated in a		areas, as appropriate.	
	near real-			
	time basis		5.1.5 The (b) (7)(E) program achieves	
	based on		cost-effective IT security objectives	
	changes in		and goals and influences decision	
	business/mi		making that is based on cost, risk, and	
	ssion		mission impact.	
	requirement			
	s and a			
	changing			
	threat and			
	technology			
	landscape.			

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



INFORMATION SECURITY TECHNICAL VULNERABILITY ASSESSMENT

For the Bureau of Indian Affairs

Report No.: 2016-ITA-021-A October 2016



OCT 0 6 2016

Memorandum

To:

Thomas Hoyler

Chief Information Security Officer, Bureau of Indian Affairs

From:

Jefferson Gilkeson Jefferson Yulean Director, Information Technology Audits Unit

Subject:

Information Security Technical Vulnerability Assessment – Bureau of Indian

Affairs

Report No.: 2016-ITA-021-A

The Office of Inspector General is assessing the effectiveness of cyber security defense measures for its evaluation of the U.S. Department of the Interior's (DOI) "Logical and Physical Security Controls at the (b) (7)(E) (2016-ITA-021). During our technical testing, we identified potential security weaknesses in the Bureau of Indian Affairs' (BIA) information technology systems. The attached report details the tests performed and the security weaknesses we identified.

As part of this evaluation, we are also performing technical testing of Bureau of Indian Education (BIE) systems that are housed at the (b) (7)(E) , including a Department designated high-value information technology asset. We will issue a separate information security technical vulnerability assessment report for any potential security weaknesses identified for BIE systems.

As this testing was part of our larger evaluation, this report contains no formal recommendations. Those findings will be part of the final evaluation report. Therefore, it is BIA's responsibility to track, evaluate, and mitigate the weaknesses we identified. Copies of this report will be provided to the BIA Director and the DOI Chief Information Officer.

If you have any questions about this report, please contact me at 703-487-5357. You may also contact Morgan Reynolds, Team Lead, at (b) (6) @doioig.gov or 703-487-5388.

Table of Contents

Introduction	I
Scope and Methodology	2
Discovery and Assessment	2
Findings	4
Hardware Asset Management	4
Inventory Best Practices	4
Software Asset Management	4
Unsupported Products	5
Vulnerability Management	5
Critical Vulnerabilities	6
Other Vulnerabilities	7
Configuration Settings Management	7
USGCB Compliance	8
CIS Best Practices	8
Configuration Issues	8
BIA Continuous Monitoring Program Plan	8
Conclusion	9
Appendix 1: Glossary	. 10
Appendix 2: Findings in Detail	. 12
Additional Details	. 12
Appendix 3: Initial Scope	. 13
BIA Identified Internal IP Address Ranges	. 13
BIA Internal Systems.	. 13

Introduction

The Office of Inspector General (OIG) is currently conducting an evaluation to assess the logical and physical security controls at the Bureau of Indian Affairs (BIA) (b) (7)(E)

Between the dates of April 25, 2016, and April 29, 2016, we conducted onsite vulnerability testing at BIA offices located in Albuquerque, NM. We performed the tests on computer and network equipment included in the occupant accreditation boundary, as well as local system and agency support workstations.

Prior to testing, we created a Rules of Engagement (ROE) document to govern the terms of the assessment activities, which was reviewed and approved by BIA. Our work was limited to noninvasive testing and was based on information provided by BIA.

The purpose of the vulnerability assessment was to ensure that BIA is implementing a detailed Information Security Continuous Monitoring (ISCM) program to enable system owners to make accurately informed risk decisions. Continuous Monitoring is defined as "maintaining ongoing awareness to support organizational risk management decisions."

This report is intended solely for BIA's internal technical review and evaluation. Due to the sensitive nature of the contained data, this report is not intended for external publication. This information is being distributed prior to release of the evaluation report to allow the Bureau to analyze and respond to these technical findings. This review does not, nor is it intended to, identify all potential vulnerabilities on all systems. This report is written for a technical audience to improve the ISCM implementation at BIA.

As part of this evaluation, we will also perform technical testing of Bureau of Indian Education (BIE) systems that are hosted at the performance including a Department designated high-value information technology asset. We will issue a separate information security technical vulnerability assessment report for any potential security weaknesses identified for BIE systems.

Appendix 1 contains a glossary of technical terms.

¹ Definition from the National Institute of Standards and Technology (NIST) SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations."

Scope and Methodology

Our work focused on four ISCM capabilities: Hardware Asset Management, Software Asset Management (including malware and patch management), Vulnerability Management, and Configuration Setting Management. We developed scripts and network tests to obtain system specific data and then compared our results with the data in the U.S. Department of the Interior's (DOI) (b) (7)(E)

is a software-based solution that allows DOI to automate Continuous Diagnostic and Mitigation (CDM) capabilities in near real time for monitoring and reporting. DOI has partnered with the U.S. Department of Homeland Security (DHS) to implement across all of its endpoints to fortify network and system cybersecurity.

The specific procedures used onsite were described in the ROE Addendum and were based only on the information made available through April 29, 2016. See Appendix 2 for specific details regarding the scope of testing activities. We were careful not to cause information system outages for BIA users or negatively impact service and staff. For this reason, we were not able to fully validate all findings and will rely on BIA staff to evaluate for mitigation activities.

Discovery and Assessment

We based initial assessment targets on a range of IP addresses and an inventory of networks provided by BIA for the system. This initial list is located in Appendix 3. Using this list of assets on the network, we performed automated Nessus scans with an advanced default safe scan policy.² As a result, we found responding IP addresses on the network.

The Nessus scanner logged into the devices with administrative credentials to verify software versions and identify vulnerabilities. Using administrative privileges, we also performed configuration testing by manually logging into random workstations and servers connected via the defined networks (see Appendix 3). We used the (b) (7)(E) on all tested machines with (b) (7)(E) ³ We continued our tests with custom scripts to review the local configuration of each machine.

² Nessus is a remote, security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer connected to a network. http://www.tenable.com/products/nessus-vulnerability-scanner

³ (b) (7)(E)

We reviewed the results from the automated Nessus scans and the locally run script utilities for relevancy and accuracy and noted several vulnerabilities and concerns. The IP addresses, additional host information, and detailed findings are listed in Appendix 2.

Findings

The weaknesses identified during testing are organized into separate categories. Appendix 2 includes a detailed list of findings that were shared with BIA staff. Each finding is organized by ISCM area and then separated into tabs. Appendix 2 also contains machine-specific details regarding each weakness, the vulnerable hosts, and weakness resolution suggestions.

Hardware Asset Management

The fundamental theory of Hardware Asset Management is that only authorized and controlled devices are allowed on the network. A complete inventory is an important control that allows an organization to verify that all of its assets undergo continuous monitoring.

Inventory Best Practices

We reviewed DOI's chosen inventory solution, In 2014, DHS mandated that CDM tools be used to create an asset list that can be automatically reported to future governmentwide ISCM dashboards. DOI has partnered with DHS to provide to all bureaus. We reviewed compliance reports and found that 22 machines of the 185 tested (approximately 12 percent) were not being monitored via Currently, DOI requires bureau participation to load agents on 100 percent of supported workstations, servers, and devices. BIA determined that it will use the solution, in addition to other solutions, for its ISCM control monitoring as specified in its continuous monitoring program plan.

Software Asset Management

Software Asset Management provides an organization with visibility into the software installed and operating on its networks and devices so the organization can appropriately manage authorized software and remove unauthorized software. All software must be configured securely and managed in the organization to ensure it is operating correctly for the role of the device it is installed on. The software profile includes authorized firmware, software products, and executable files for the associated device roles. Authorized software should be added to a whitelist of software products and executables.

The software profile also includes blacklists of specifically prohibited software defined or identified to assist in rapid decision making during the identification and remediation process. In addition, any discovered software that is not explicitly listed on a whitelist or blacklist should be initially placed on a graylist. Software included in the graylist will either be authorized and permitted to remain installed on the device until authorization is determined, or unauthorized and required to be uninstalled until authorization is determined. Items on the graylist

⁴ https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

must be moved to either a whitelist or a blacklist within a specific timeframe to ensure that BIA continues to improve upon this capability.

Unsupported Products

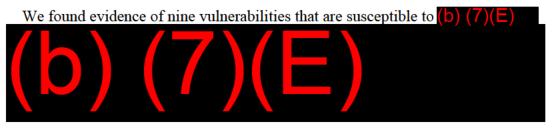
We found several products that have met their end of life. These software products should be added to the blacklist and removed from all machines as soon as possible because they are no longer supported. We discovered (b) (7)(E) software products that were out of date. Unsupported software packages often create vulnerabilities that cannot be mitigated, so discontinuing use of unsupported and out-of-date products is critical.

Vulnerability Management

The ability to search for and identify all software products on installed networks, combined with the ability to identify vulnerabilities or weaknesses associated with those software products is known as vulnerability management. Known vulnerabilities are those with a common vulnerability exposure (CVE) identifier.⁵

Attackers continually scan devices for known vulnerabilities that can be exploited to gain a foothold into a network. Once a foothold is secured, attackers can exfiltrate sensitive data or launch additional attacks deeper into the network. Attackers also attempt to exploit known vulnerabilities using additional attack vectors such as malicious emails, Web browser redirects, or executing embedded software code in the email itself.

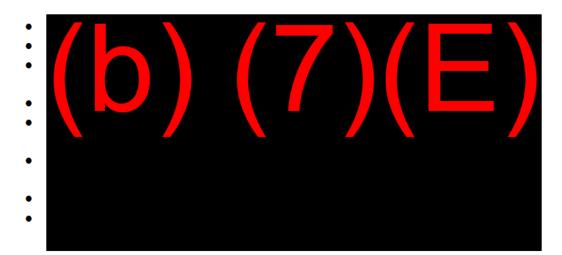
We used Nessus to conduct our vulnerability assessment. It is considered a best practice to scan all network ranges with elevated account credentials to discover vulnerabilities and insecure configuration settings. We deemed weaknesses in this category to be of the highest priority for BIA evaluation and resolution. We placed these weaknesses into this category after our review based on a combination of testing utility recommendations, impact, CVE scores, and auditor experience.



• (b) (7)(E)

⁵(b) (7)(E) ⁶(b) (7)(E)

Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.



Critical Vulnerabilities

(b) (7)(E)

We observed servers susceptible to the (b) (7)(E) at BIA. This can be remediated by patching the affected software or upgrading to unaffected versions.

(b) (7)(E)

We observed four systems running the (b) (7)(E)
(b) (7)(E), which is inherently vulnerable to (b) (7)(E)
(b) (7)(E)
This capability should be disabled on these systems.

(b) (7)(E)

We observed servers running (b) (7)(E) , including a combined (b) (7)(E) vulnerabilities across these servers. Every instance had an outdated and vulnerable instance of (b) (7)(E) with (b) (7)(E). All vulnerabilities can be remediated by updating (b) (/)(E) to the latest build.

(b) (7)(E

We observed vulnerability instances across hosts running (b) (7)(E). (b) (7)(E) were represented in the vulnerabilities. These vulnerabilities can be resolved by upgrading to the latest version of (b) (7)(E)

(b) (7)(E

We observed vulnerabilities across hosts running (b) (7)(E)

These vulnerability instances (b) (7)(E)

All instances can be resolved by upgrading to the latest version of (b) (7)(E)

(b) (7)(E)

We observed vulnerabilities affecting (b) (7)(E)

(b) (7)(E)

These vulnerabilities are spread across hosts. Of these

vulnerabilities can be resolved by applying patches that (b) (7)(=) (b) (7)(E) We observed a vulnerability on (b) (7)(E) host systems relating to (b) (7)(t) (a) (7)(E). This vulnerability can be remediated by updating (b) (7)(E) to the latest build. (b) (7)(E) We observed instances of vulnerabilities on (b) (7)(= workstations and servers. We found unique vulnerabilities with patches available including some from category includes all (b) (7 patching and maintenance. The issue with keeping (b) (7)(= appears to be common across DOI, but still needs to be addressed. We identified . Of those vulnerabilities on hosts with (b) (7)(=) vulnerabilities. (b) (7)(E) can be remediated by updating (b) (7) The vulnerabilities related to outdated (b) vulnerabilities related to outdated (b) (7)(= Other Vulnerabilities Medium Findings

These findings are provided for your information and should be reviewed after the more critical items are addressed. We discovered these findings using the same processes described, and they have a lower priority due to mitigation control responsibilities and possible impact.

(b)(/)(E)

We found that BIA did not keep (b) (7)(=) updated. Although b) (7) is patched at the (b) (7)bureaus need to maintain an active role in ongoing patching and maintenance.

Other Potential Vulnerabilities

We included other vulnerabilities in our report to notify BIA of other potential vulnerabilities to look into.

Configuration Settings Management

The desired state of workstation configuration should be monitored for compliance to ensure the device is within secure operating ranges while in use. We asked DOI and BIA to provide (b) (7)(E) , and then used automated tools to determine whether the devices were adequately inventoried and configured.

USGCB Compliance

USGCB provides a standard security configuration baseline for Microsoft Windows 7 operating systems and Microsoft Internet Explorer web browsers. USGCB clarifies configurations for the Federal Desktop Core Configuration (FDCC). There are possible USGCB recommended common configurations for the Microsoft Windows 7 operating system. All Microsoft systems tested were (b) (7)(E) workstations and (b) (7)(E) servers. There are currently no official Government baselines for these operating systems.

CIS Best Practices

Using a Center for Internet Security (CIS) benchmark tool, we assessed the security of servers against industry consensus-based, best practice configuration settings that are not included in the USGCB standard. When we ran the CIS tool on (b) (7)(E) servers and (b) (7)(E) workstations at BIA, we found that on average, the (b) (7)(E) were percent compliant and the Windows workstations were percent compliant. One setting BIA deviated (b) (7)(E)

Configuration Issues

We identified issues such as devices configured with (b) (7)(E)

(b) (7)(E) and other settings that need to be reviewed for the security of the information systems.

BIA Continuous Monitoring Program Plan

We found that BIA had a well-documented, continuous monitoring plan that details how will be used to continuously monitor configuration management items. BIA will need management support to ensure appropriate, risk-based decisions are being made on accurate and near real-time data. As defined by BIA, all of these controls require coordination with other tools and in-depth technical review. As it stands, these disparate monitoring solutions are not currently capable of providing a single point of real-time risk analysis to system owners.

⁷ USGCB and FDCC configuration setting were developed by the U.S. Department of Defense (DoD) with the assistance of NIST and related IT vendors. http://usgcb.nist.gov/index.html

Conclusion

We found several concerns based on our technical testing; some of the most critical were related to patching, configuration, and inventory management. We



BIA should evaluate and mitigate the results. As this testing was a step of OIG's larger evaluation of "Logical and Physical Security Controls at the (b) (7)(E) (2016-ITA-021), this report contains no formal recommendations. These findings will be part of the final evaluation report. The tracking, evaluation, and mitigation of the identified weaknesses in this report are the responsibility of BIA.

For questions or clarification regarding further analysis or mitigation options, please contact Morgan Reynolds at 703-487-5388.

Appendix I: Glossary

CDM, Continuous Diagnostic and Mitigation

A U.S. Department of Homeland Security (DHS) program to fortifying the cybersecurity of Government networks and systems by offering modernized, commercial, off-the-shelf software to agencies. CDM provides agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cyber security personnel to mitigate the most significant problems first. Summary information from a CDM tool can feed into an enterprise level dashboard to inform and provide situational awareness data across the Federal Government (www.dhs.gov/cdm).

DOI CIRC, U.S. Department of the Interior's Computer Incident Response Center An entity that provides DOI and its bureaus with computer security related incident response capabilities. DOI CIRC coordinates threat identification and incident remediation with the U.S. Computer Emergency Readiness Team (USCERT).

False Positive

An instance in which a security tool incorrectly classifies benign content as malicious, or an alert that incorrectly indicates that a vulnerability is present.

Firewall

Software or a system or gateway that can protect a computer or network from other networks by limiting and monitoring network communication.

Incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Intrusion Detection

The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents; which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

IDS, Intrusion Detection System

Software that automates the identification of possible incidents.

IPS, Intrusion Prevention System

Software that has all of the capabilities of an IDS and can also attempt to stop possible incidents.

ISCM, Information Security Continuous Monitoring

An agency program to enable ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

ROE, Rules of Engagement

Documentation of boundaries that specify a clearly defined scope for testing or attacking a specific environment.

Security Control

A protective measure for a system against threats.

Vulnerability/Weakness

A flaw or weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

Vulnerability Scanning

Also known as vulnerability analysis, vulnerability assessment, or vulnerability testing; this process defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure.

Appendix 2: Findings in Detail

The weaknesses that resulted in each finding are described in terms of exploitation requirements and potential impacts. The attached file provides BIA technical staff with detailed documentation of our findings.

Additional Details

Several aspects of identified weaknesses may be larger than can be reasonably detailed in the description. Other aspects, including initial target scope and discovered services, are included as well.

Appendix 3: Initial Scope

BIA Identified Internal IP Address Ranges



Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



INFORMATION SECURITY TECHNICAL VULNERABILITY ASSESSMENT

For the Bureau of Indian Education

Report No.: 2016-ITA-021-B October 2016



OCT 1 7 2016

Memorandum

To: Thomas Hoyler

Chief Information Security Officer, Bureau of Indian Affairs

From:

Jefferson Gilkeson Jefferson Yuken Director, Information Technology Audits Unit

Subject: Information Security Technical Vulnerability Assessment – Bureau of Indian

Education

Report No.: 2016-ITA-021-B

The Office of Inspector General is assessing the effectiveness of cyber security defense measures for its evaluation of the U.S. Department of the Interior's (DOI) "Logical and Physical " (2016-ITA-021). During our technical Security Controls at the (b) (7)(E) testing, we identified potential security weaknesses in the Bureau of Indian Education's (BIE) information technology (IT) systems. Our tests were limited to the responding IP addresses detected as part of our discovery scans because the (b) (7)(E) IT staff did not provide complete address ranges for all BIE IT assets at the time of our testing. The attached report details the tests performed and the security weaknesses we identified. We issued a separate technical vulnerability assessment report for potential security weaknesses identified for Bureau of Indian Affairs systems at the (b) (7)(E)

As this testing was part of our larger evaluation, this report contains no formal recommendations. Our final evaluation report will contain our findings and recommendations. Therefore, BIE is responsible for tracking, evaluating, and mitigating the identified weaknesses. We are providing copies of this report to the BIE Director and the DOI Chief Information Officer.

If you have any questions about this report, please contact me at 703-487-5357. You may also contact Morgan Reynolds, Team Lead, at (b) (6) @doioig.gov or 703-487-5388.

Table of Contents

Introduction	1
Scope and Methodology	2
Discovery and Assessment	2
Findings	4
Hardware Asset Management	4
Inventory Best Practices	4
Software Asset Management	4
Unsupported Products	4
Vulnerability Management	5
Critical Vulnerabilities	5
Other Vulnerabilities	7
Configuration Settings Management	7
USGCB Compliance	8
CIS Best Practices	8
Configuration Issues	8
(b) (7)(E)	8
(b) (7)(E)	9
BIE Continuous Monitoring Program Plan	9
Conclusion	. 10
Appendix 1: Glossary	. 11
Appendix 2: Findings in Detail	. 13
Additional Details	. 13
Appendix 3: Initial Scope	. 14
RIF Identified Internal IP Address Ranges	14

Introduction

The Office of Inspector General (OIG) is conducting an evaluation to assess the logical and physical security controls at the Bureau of Indian Education (BIE)

(b) (7)(E)

(b) (7)(E)

From April 25, 2016 to April 29, 2016, and June 28 2016 to June 29, 2016, we conducted onsite vulnerability testing at BIE offices in Albuquerque, NM. We performed the tests on computer and network equipment included in the BIE and accreditation boundaries, as well as local system and agency support workstations.

Prior to testing, we created a Rules of Engagement (ROE) document to govern the terms of the assessment activities, which the Bureau of Indian Affairs (BIA) reviewed and approved. Our work was limited to noninvasive testing, based on information provided by BIE.

The purpose of the vulnerability assessment was to ensure that BIE is implementing a detailed Information Security Continuous Monitoring (ISCM) program to enable system owners to make accurately informed risk decisions. Continuous Monitoring is defined as "maintaining ongoing awareness to support organizational risk management decisions."

This report is intended solely for BIE's internal technical review and evaluation. Due to the sensitive nature of the contained data, this report is not intended for external publication. We are distributing this information prior to our evaluation report to allow the Bureau to analyze and respond to our technical findings. This review does not, nor is it intended to, identify all potential vulnerabilities on all systems. This report is written for a technical audience to improve the ISCM implementation at BIE.

Appendix 1 contains a glossary of technical terms.

FOR OFFICIAL USE ONLY

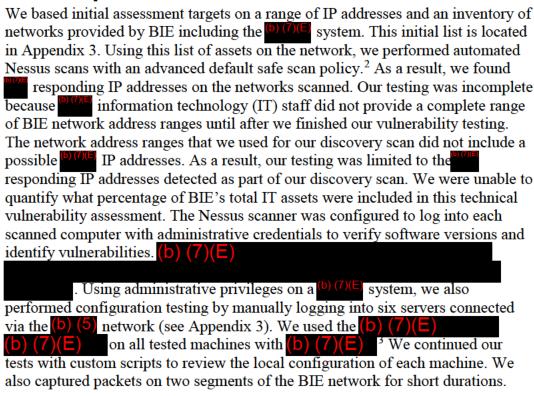
Definition from the National Institute of Standards and Technology (NIST) SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations."

Scope and Methodology

Our work focused on four ISCM capabilities: Hardware Asset Management, Software Asset Management (including malware and patch management), Vulnerability Management, and Configuration Setting Management. We developed scripts and network tests to obtain system-specific data.

The specific procedures used onsite were described in the ROE and were based only on the information made available through June 29, 2016. See Appendix 2 for specific details regarding the scope of testing activities. We were careful not to cause information system outages for BIE users or negatively impact service and staff. For this reason, we were not able to fully validate all findings and will rely on BIE staff to evaluate for mitigation activities.

Discovery and Assessment



² Nessus is a remote, security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer connected to a network (http://www.tenable.com/products/nessus-vulnerability-scanner).

⁽b) (7)(E)

We reviewed the results from the automated Nessus scans, the locally run script utilities and the packet captures for relevancy and accuracy and noted several vulnerabilities and concerns. The IP addresses, additional host information, and detailed findings are listed in Appendix 2.

Findings

The weaknesses identified during testing are organized into separate categories. Appendix 2 includes a detailed list of findings shared with BIE staff. Each finding listed in the appendix is organized by ISCM area and then separated into tabs. Appendix 2 also contains machine-specific details regarding each weakness, the vulnerable hosts, and weakness resolution suggestions.

Hardware Asset Management

The fundamental theory of Hardware Asset Management is that only authorized and controlled devices are allowed on the network. A complete inventory is an important control that allows an organization to verify that all of its assets undergo continuous monitoring.

Inventory Best Practices

We reviewed DOI's chosen inventory solution, (b) (7)(E) In 2014, the U.S. Department of Homeland Security (DHS) mandated that Continuous Diagnostics and Mitigation (CDM) tools be used to create an asset list that can be automatically reported to future governmentwide ISCM dashboards. DOI has partnered with DHS to provide (b) (7)(E) to all bureaus. (b) (7)(E) is not installed on any BIE systems. The BIE systems are on a separate network so they cannot reach the DOI (b) (7)(E) console. BIE intends to install a separate BIE (b) (7)(E) instance; however, that work was not completed at the time of our assessment. Currently, DOI requires bureau participation to load (b) (7)(E) agents on 100 percent of supported workstations, servers, and devices.

Software Asset Management

Software Asset Management provides an organization with visibility into the software installed and operating on its networks and devices so the organization can appropriately manage authorized software and remove unauthorized software. All software must be configured securely and managed in the organization to ensure it is operating correctly for the role of the device it is installed on. The software profile includes authorized firmware, software products, and executable files for the associated device roles.

Unsupported Products

We found instances of software product installed on BIE computers that are unsupported by vendors. These software products should be added to the blacklist and removed from all machines as soon as possible because they are no longer supported. We discovered software products on computers that were outdated. Unsupported software packages often create vulnerabilities that cannot

⁴ https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf

be mitigated, so discontinuing the use of unsupported and outdated products is critical.

Vulnerability Management

The ability to search for and identify all software products on installed networks, combined with the ability to identify vulnerabilities or weaknesses associated with those software products is known as vulnerability management. Known vulnerabilities are those with a common vulnerability exposure (CVE) identifier.⁵

Attackers continually scan devices for known vulnerabilities that can be exploited to gain a foothold into a network. Once a foothold is secured, attackers can exfiltrate sensitive data or launch additional attacks deeper into the network. Attackers also attempt to exploit known vulnerabilities using additional attack vectors such as malicious emails, Web browser redirects, or executing embedded software code in the email itself.

Scanning all network ranges with elevated account credentials to discover vulnerabilities and insecure configuration settings is considered a best practice. Using Nessus to conduct our vulnerability assessment, we placed these weaknesses into categories after our review based on a combination of testing utility recommendations, impact, CVE scores, and auditor experience. We deemed such identified weaknesses to be of the highest priority for BIE evaluation and resolution.



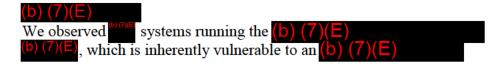
Critical Vulnerabilities

(b) (7)(E

We observed instances of the vulnerability on BIE servers susceptible to the vulnerability. This can be remediated by patching the affected software or upgrading to unaffected versions.

(b) (7)(E)

We observed instances of the Heartbleed vulnerability on systems at BIE. This can be remediated by patching the affected SSL implementations.



⁵ https://cve mitre.org/

We observed vulnerabilities across hosts running (b) (7)(E) All instances can be resolved by upgrading to the latest version of We observed vulnerabilities across hosts running (b) (7) These vulnerable instances cover (b) (7)(E) All instances can be resolved by upgrading to the latest version of vulnerabilities on (b) (7)(E) host systems relating to We observed and (b)(7)(E)All vulnerabilities can be remediated by instances of vulnerabilities on (b) (7) We observed workstations and servers. Of the instances of vulnerabilities we found, , and one dated (b) (7)(E) were over (b) (7)were unique, (b) (7)(E) and (b) (7)(E We observed instances on hosts with vulnerable instance of (b) (1)(E). In addition, we observed instances on hosts with vulnerable instances of We observed (b) (7)(E) systems with critical vulnerabilities. Upgrading will remediate these vulnerabilities. category includes all (b) (7) , which require regular patching and maintenance. The issue with keeping (b) (7)(E) appears to be common across DOI, but still needs to be addressed. We identified (a) (b) (7)(E) vulnerabilities on hosts with unique CVEs. Removing or patching (b) (7)(E) would remediate all vulnerabilities. Also, were related to (b) (7)(E) , and vulnerabilities were related to (b) (7)(E)

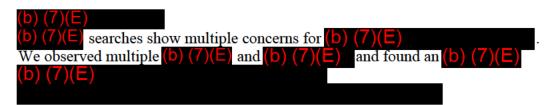
Other Vulnerabilities

Medium Findings

These findings are provided for your information and should be reviewed after the more critical items are addressed. We discovered these findings using the same processes described in this report. These findings have a lower priority due to mitigation control responsibilities and potential impact.

(b) (7)(E) servers were not scanned with administrative credentials before this review. We requested 3 months of historical scans from the support personnel. They were only able to provide a single scan dating a week prior to our initial visit in April. That report confirmed the lack of administrative credentials used during (b) (7)(E) testing. We learned that BIE did not have administrative access to the (b) (7)(E) servers before our request to scan that network. (b) (7)(E) contractors stated they fully patched eight (b) (7)(E) servers (only the computers they expected us to scan) on June 26, 2016. Even with this patching, our scans still showed two machines with critical findings. We were unable to scan two machines because the credentials provided were not valid. During a phone call, (b) (7)(E) contractors stated that they were unaware of any security requirements they needed to meet.

Confusion also appears to surround BIE's inventory of networks and devices. We are not certain that BIE has completed a start-to-finish scan of the BIE class B networks. In addition, we found that BIE's vulnerability management tool, had instances of products that need critical patches. hosts had with critical vulnerabilities. The endpoint protection tools should never introduce vulnerabilities on the networks they are protecting.



We found (b) (7)(E)

Configuration Settings Management

The desired state of workstation configuration should be monitored for compliance to ensure the device is within secure operating ranges while in use. We asked DOI and BIE to provide all (b) (7)(E)

, and then used automated tools to determine whether the devices were adequately inventoried and configured. (7)(E) Compliance provides a standard security configuration baseline for Microsoft Windows 7 operating systems and Microsoft Internet Explorer web browsers. b) (7)(E) clarifies configurations for the Federal Desktop Core Configuration (FDCC). 6 There are possible possible recommended common configurations for the Microsoft Windows 7 operating system. All Microsoft systems tested were servers. Currently, no official Government baselines exist for this operating system. **CIS Best Practices** Using a Center for Internet Security (CIS) benchmark tool, we assessed the security of servers against industry consensus-based, best practice configuration settings that are not included in the (b) (7)(E) standard. When we ran the CIS tool on six (b) (7)(E) Windows servers at BIE, we found that on average, the Windows percent compliant. In addition, the machines are (b) (7)(E) servers were (b) (7)(E) as determined by our scripts. GPO's are typically used by administrators to apply the same approved policies across multiple servers. Configuration Issues We identified issues such as devices configured with (b) (7) These items need to be reviewed for the security of the information systems. We captured packets on the BIE network for more than 24 hours using standard and custom (b) (7)(E) . Due to storage limitations, our device was configured to only store packets associated with an IDS signature. We found that BIE has not (b) (7)(E) on its general support system and two moderate impact systems, (b) (7)(= result of the OMB CyberSprint activity in 2015 and direction provided by OMB as part of that effort, in April 2015 DOI accelerated the rollout of to systems across the Department. In September 2015, DOI reported that 100 percent of its computer systems (b) (7)(= . Computer systems that (b) (7)(E) are far more secure than systems

and FDCC configuration setting were developed by the U.S. Department of Defense (DoD) with the assistance of NIST and related IT vendors. http://usgcb.nist.gov/index.html

```
breaches, including the 2015 U.S. Office of Personnel Management data breach,
could have been prevented with multifactor authentication in place. Full
implementation of multifactor (b) (7)(E)
We found that (b)(7)(E)
                            BIE's servers used the (b) (7)(E)
                                                                 to manage
                                 . The (b) (7)(E)
                                                            . Our logs indicated
     BIE servers (b) (7)(E)
We also found that (b) (7)(=)
                                                                        . We
identified (b) (7)(L)
                    instance where a (b) (7)(E) server was (b) (7)(E)
Lastly, we found
We found that the Bureau of Indian Affairs (BIA) a well-documented,
(b) (7)(E)
                                                          will need
management support to ensure an (b) (7)(E) instance is built, installed, and
maintained so the (b) (7)(E)
                                                  . We found that (b) (7)(E)
                                   but the System Security Plan for (b) (7)(t
stated the (b) (7) (E)
                                            . During interviews we asked about
the documentation and ISSO for (b) (7)(E) The BIA CISO stated that the position
has not been filled for at least 2 years. Also, the Contracting Officer's Technical
Representative (COTR) and the contractor do not believe the current
contract includes security requirements.
```

Conclusion

We found several concerns based on our technical testing, with the most critical related to patching, configuration, and inventory management. We identified a large number of missing patches, including (b) (7)(E)

(b) (7)(E)

(b) (7)(E) is not installed on any BIE systems. We also found (b) (/)(E)

In addition, our tests were limited as we were not provided the network address ranges for all BIE IT assets in (b) (7)(E)

BIE should evaluate and mitigate the results. As this testing was part of OIG's larger evaluation of "Logical and Physical Security Controls at the Albuquerque Data Center" (2016-ITA-021), this report contains no formal recommendations. These findings will be part of the final evaluation report. The tracking, evaluation, and mitigation of the identified weaknesses in this report are the responsibility of BIE.

For questions or clarification regarding further analysis or mitigation options, please contact Morgan Reynolds at 703-487-5388.

Appendix I: Glossary

CDM, Continuous Diagnostic and Mitigation

A U.S. Department of Homeland Security (DHS) program to fortifying the cybersecurity of Government networks and systems by offering modernized, commercial, off-the-shelf software to agencies. CDM provides agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cyber security personnel to mitigate the most significant problems first. Summary information from a CDM tool can feed into an enterprise level dashboard to inform and provide situational awareness data across the Federal Government (www.dhs.gov/cdm).

DOI CIRC, U.S. Department of the Interior's Computer Incident Response Center An entity that provides DOI and its bureaus with computer security related incident response capabilities. DOI CIRC coordinates threat identification and incident remediation with the U.S. Computer Emergency Readiness Team (USCERT).

False Positive

An instance in which a security tool incorrectly classifies benign content as malicious, or an alert that incorrectly indicates that a vulnerability is present.

Firewall

Software or a system or gateway that can protect a computer or network from other networks by limiting and monitoring network communication.

Incident

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices.

Intrusion Detection

The process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents; which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices.

IDS, Intrusion Detection System

Software that automates the identification of possible incidents.

IPS, Intrusion Prevention System

Software that has all of the capabilities of an IDS and can also attempt to stop possible incidents.

ISCM, Information Security Continuous Monitoring

An agency program to enable ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

ROE, Rules of Engagement

Documentation of boundaries that specify a clearly defined scope for testing or attacking a specific environment.

Security Control

A protective measure for a system against threats.

Vulnerability/Weakness

A flaw or weakness in system security procedures, design, implementation, internal controls, etc., that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.



Appendix 2: Findings in Detail

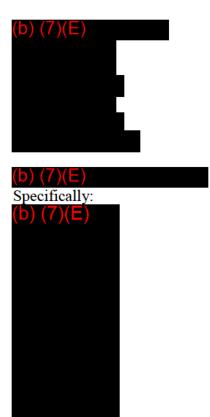
The weaknesses that resulted in each finding are described in terms of exploitation requirements and potential impacts. The attached file provides BIE technical staff with detailed documentation of our findings.

Additional Details

Several aspects of identified weaknesses may be larger than can be reasonably detailed in the description. Other aspects, including initial target scope and discovered services, are included as well.

Appendix 3: Initial Scope

BIE Identified Internal IP Address Ranges



Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



For Official Use Only

This report may contain information subject to the Freedom of Information Act, 5 U.S.C. § 552.

Report No.: ISD-AT-BOR-0002-2012



MAR 2 9 2013

Memorandum

To:

Michael L. Connor

Commissioner, Bureau of Reclamation

From:

Donald W. Cairns

Deputy Assistant Inspector General

Office of Audits, Inspections, and Evaluations

Subject:

Final Inspection Report – IT Security of the (b) (7)(E) Dam (b) (7)(E)

Report No. ISD-AT-BOR-0002-2012

We recently completed an inspection of (b) (7)(E) Dam's (b) (7)(E) . Our objective was to assess the Bureau of Reclamation's (USBR) security posture for its (b) (7)(E). To accomplish this objective, we—

- obtained a general understanding of (b) (7)(E) programs managed by USBR;
- visited (b) (7)(E) Dam and interviewed officials from numerous programs in the dam's operations;
- reviewed documentation and internal reports provided by USBR staff;
- ascertained if the (b) (7)(E) network infrastructure was isolated from other U.S. Department of the Interior (DOI) business networks and the Internet;
- examined the effectiveness and efficiency of the continuous monitoring of the cyber assets that manage (b) (7)(E) Dam; and
- determined whether additional security controls could bolster (b) (7)(E) Dam's overall information technology (IT) security.

We conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

(b) (7)(E) Dam's (b) (7)(E) system was adequately air-gapped, thus properly isolated from the Internet. Isolation from Internet user traffic insulates the system from the USBR and DOI business networks, thus decreasing the risk to the system from Internet-based exploitations. We found, however, that the system had limited and inefficient continuous monitoring, no automated safeguards in mobile media controls and enforcement, only single factor authentication for physical facility access and logical system access, and that the system categorization was miscategorized as moderate.

Office of Audits, Inspections, and Evaluations | Washington, DC

We make five recommendations to strengthen the security posture of (b) (7)(E) Dam's (b) (7)(E) system. Our recommendations, if implemented, should improve controls surrounding the system.

Background

Critical infrastructure and cyber systems continue to rely on IT for essential operations. Protecting the infrastructure from cyber threats remains a top priority. Historically, critical infrastructures' cyber element was somewhat protected due to the lack of information on it; however, this anonymity is disappearing quickly with the growing connectivity of systems to the Internet. Recent U.S. Department of Homeland Security (DHS) warnings indicate that the threat to industrial control systems controlling our critical infrastructure is increasing.

Results of Inspection

Minimizing network exposure for the (b) (7)(E) was our primary focus. We found the system was not directly connected to the Internet and not connected to the Department's or USBR's business networks. Connections we did find were documented with interconnection security agreements and network diagrams. We found, however, some control areas that could present risks to the system.

Continuous Monitoring

USBR has not fully achieved a comprehensive, integrated continuous monitoring control program for Dam's (b) (7)(E). Continuous monitoring is required by the Federal Information Security Management Act of 2002, Office of Management and Budget and, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37.

The system does not currently utilize an automated continuous monitoring program. Risk factors and an understanding of a system's security controls are gained through continuous monitoring and near-real-time event alerting. Instead, USBR manually reviews the IT security logs on a weekly basis, which is time consuming and tedious. In addition, we found that the IT security logs were reviewed by the same personnel responsible for maintaining the system, even though the properties of Dam has an onsite IT security manager who could perform the reviews. Separation of duties is essential in preventing and detecting malevolent activities. Also, the lack of adequate separation of duties does not conform to the mandates prescribed in NIST SP 800-53.

Mobile Media Safeguards

While managerial policies are in place that restrict the usage of mobile media devices, the Dam's (b) (7)(E) and did not have an automated technical enforcement or monitoring capability. Altogether, the system manages three dams, (b) (7)(E) classified as NCI, and which are both categorized as Major Mission Critical (MMC). The lack of mobile media controls across this expanded footprint could allow the introduction of malicious components (malware and viruses) into the system via mobile media devices (thumb drives, optical discs, or portable hard drives).

Physical Facility Access

Considering the volume of tourists and visitors to Dam, coupled with single-factor authentication and no guards at the entrances, physical security may be vulnerable to badge and card-reader weaknesses. For example, if a dam employee loses his or her card, anyone who finds the card would have access to the facility.

Logical System Access

We found that USBR is using single-factor authentication (username and password) for system login. Two-factor authentication, as required by Homeland Security Presidential Directive 12 (HSPD-12), and Federal Information Processing Standard 201(FIPS-201), enhances identity management and facilitates strong information system authentication.

System Categorization

We believe that (b) (7)(E) Dam's (b) (7)(E) was incorrectly categorized as a "Moderate Impact" system. The requisite level of system protection, security controls, and risk assessments are all determined by system categorization. A miscategorization could lead to an incomplete implementation of Federal guidance. It could also affect most of the system's certification and accreditation documents.

Based on the guidance contained in Federal Information Processing Standards 199, NIST SP 800-30, and NIST SP 800-60, the system should be categorized as "High Impact." The guidance defines a high-impact system as a system that if lost would result in having "severe or catastrophic adverse effects that could result in severe or catastrophic harm to individuals including the loss of life or serious life threatening injuries." In this regard, (b) (7)(E) Dam's should have be categorized as a "High Impact" because—

- there is potential endangerment to life and property;
- the system not only has management and control for (b) (7)(E) Dam, which is classified as NCI, but also two other dams classified as MMC;
- USBR considers the dams vital to national security, economics, public health or safety, and high downstream hazards;

- the cyber systems that control the electrical generation and water flow at (b) (7)(E) Dam are also designated as NCI; and
- there are many downstream impacts considering numerous compacts, Federal laws, court decisions and decrees, contracts, and regulatory guidelines known as the "Law of the River." These include
 - o the Mexican Water Treaty of 1944;
 - o the Colorado River Compact of 1922;
 - o the California Seven Party Agreement of 1931;
 - o the Upper Colorado River Basin Compact of 1948;
 - o the Colorado River Storage Project of 1956; and
 - o the Arizona v. California U.S. Supreme Court Decision of 1964.

Recommendations

We make five recommendations based upon our findings.

- 1. Design and implement an automated, continuous monitoring program for Dam's (b) (7)(E) that includes appropriate separation of duties.
- 2. Implement automated monitoring and enforcement of required mobile media security controls.
- 3. Implement two-factor authentication that requires electronic card and a keyed pin number for physical access to (b) (7)(E) Dam.
- 4. Implement two-factor authentication that requires an electronic card and a typed password to log into the (b) (7)(E) system.
- 5. Categorize (b) (7)(E) Dam's (b) (7)(E) as "High Impact" and implement required controls according to this categorization.

Please provide us with your written response to this report within 30 days. The response should provide information on actions taken or planned to address the recommendations, as well as target dates and title(s) of the official(s) responsible for implementation. Please send your response to:

Donald W. Cairns U.S. Department of the Interior Office of Inspector General Mail Stop 4428 1849 C Street, NW. Washington, DC 20240

If you have any questions regarding this report, please contact me at 202-208-1454 or Roy Mills at 202-208-5724.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



INDEPENDENT AUDITORS' PERFORMANCE
AUDIT REPORT ON THE U.S. DEPARTMENT
OF THE INTERIOR FEDERAL INFORMATION
SECURITY MANAGEMENT ACT FOR FISCAL
YEAR 2013

Report No.: ISD-IN-MOA-0001-2013



Memorandum

FEB 2 6 2014

To:

Bernard Mazer

Chief Information Officer

From:

Mary L. Kendall

Deputy Inspector General

Subject:

Independent Auditors' Performance Audit Report on the U.S. Department of the

Hardall

Interior Federal Information Security Management Act for Fiscal Year 2013

Report No. ISD-IN-MOA-0001-2013

This memorandum transmits the KPMG LLP (KPMG) Federal Information Security Management Act (FISMA) audit report of the U.S. Department of the Interior (DOI) for fiscal year (FY) 2013. FISMA (Public Law 107-347) requires Federal agencies to have an annual independent audit of their information security programs and practices performed by their Office of Inspector General (OIG) or by an independent auditor, as determined by their OIG, to determine the effectiveness of such programs and practices.

KPMG, an independent public accounting firm, performed the DOI FY 2013 FISMA audit under a contract issued by DOI and monitored by OIG. As required by the contract, KPMG conducted the audit in accordance with Generally Accepted Government Auditing Standards to obtain sufficient, appropriate evidence to provide a reasonable basis for its findings and conclusions based on the audit objectives. KPMG is responsible for the findings and conclusions expressed in the audit report. OIG does not express an opinion on the report nor on KPMG's conclusions regarding DOI's compliance with laws and regulations.

FISMA reporting has been completed in accordance with Office of Management and Budget Memorandum M-14-04, "FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," dated November 18, 2013, and Homeland Security Federal Information Security Memorandum (FISM) 13-01, with the same subject, dated September 4, 2013.

KPMG reviewed information security practices, policies, and procedures at the DOI Office of the Chief Information Officer and 13 DOI bureaus and offices:

- the Bureau of Indian Affairs;
- the Bureau of Land Management;
- the Bureau of Reclamation;
- the Bureau of Safety and Environmental Enforcement;
- the U.S. Fish and Wildlife Service:

- the Interior Business Center;
- the National Park Service;
- the Office of the Secretary;
- the Office of Inspector General;
- the Office of Surface Mining Reclamation and Enforcement;
- the Office of the Special Trustee for American Indians;
- the Office of the Solicitor; and
- the U.S. Geological Survey.

To ensure the quality of the audit work, OIG—

- reviewed KPMG's approach and planning of the audit;
- evaluated the auditors' qualifications and independence;
- monitored the audit's progress at key milestones;
- observed KPMG during fieldwork site visits;
- engaged in regularly scheduled meetings with KPMG and DOI management to discuss audit progress, findings, and recommendations;
- reviewed KPMG's supporting work papers and audit report; and
- performed other procedures it deemed necessary.

KPMG concluded that, consistent with applicable FISMA requirements, Office of Management and Budget policy, and National Institute of Standards and Technology guidelines, DOI has established and maintained security programs for continuous monitoring management, identity and access management, incident and response reporting, risk management, security training, plans of action and milestones, remote access management, contractor systems, and security capital planning. KPMG identified needed improvements, however, in the configuration management and contingency planning program areas and noted that DOI bureaus and offices were not completely aware of the requirements to develop, review, or update procedures that support the DOI Information Technology Security Control Standards. KPMG made 29 recommendations intended to strengthen DOI's information security program.

OIG introduced a new method for measuring compliance in FY 2013, raising the threshold for measuring system compliance from a 50 percent standard in FY 2012 to a 70 percent standard in FY 2013. This increase should be noted when comparing compliance results from FYs 2012 to 2013. To help DOI's compliance reach 100 percent, OIG will work with the chief information officer to determine and project appropriate compliance goal increases at the beginning of FISMA reporting cycles.

In addition, OIG acknowledged that its own system represented the lowest compliance score and adversely affected the overall DOI score. The OIG system had been planned for a transition to the DOI network in FY 2013, but the transition did not occur. OIG will work with the chief information officer to transition its systems as soon as practical, which will result in improved FISMA scores.

OIG will refer KPMG's recommendations to the Office of Financial Management for audit follow-up. The legislation creating OIG requires that we report to Congress semiannually

on all audit, inspection, and evaluation reports issued; actions taken to implement recommendations; and recommendations that have not been implemented. Distribution of this report should be restricted, and the report should not be made available to the public.

We appreciate the cooperation and assistance of DOI personnel during the audit. If you have any questions regarding the report, please contact me at 202–208–5745.

Attachment

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



For Official Use Only

This report may contain information subject to the Freedom of Information Act, 5 U.S.C. § 552.

Report No.: ISD-IS-BOR-0004-2013



MAR 2 6 2014

Memorandum

To:	Lowell D. Pimle
	Acting Commiss

Acting Commissioner, Bureau of Reclamation

From: forKimberly Elmore

Assistant Inspector General for Audits, Inspections, and Evaluations

Subject: Inspection

Inspection Report – IT Security of the (b) (7)(E)

(b) (7)(E)

Report No. ISD-IS-BOR-0004-2013

(b) (7)(E) Dam is one of five Bureau of Reclamation (USBR) dams, which were identified as National Critical Infrastructure (NCI) and which require special security considerations as documented by the Department of Homeland Security (DHS). (b) (7)(E) Dam is also the key component of USBR's (b) (7)(E) to automate, manage, and protect numerous processes, functions, and operations.

We completed an inspection of the (b) (7)(E) that supports the (b) (7)(E) Dam and which operates and monitors thousands of devices at (b) (7)(E), ranging from simple temperature sensors to automated controls for generators and gate functions. Our objective was to assess the security posture for the (b) (7)(E) based on recent warnings from DHS. To accomplish this objective, we—

- obtained a general understanding of (b) (7)(E) programs managed by USBR;
- visited the (b) (7)(E) Dam and interviewed officials from numerous programs in the dam's operations;
- reviewed documentation and internal reports provided by USBR staff;
- ascertained if the (b) (7)(E) network infrastructure was isolated from other U.S. Department of the Interior (DOI) business networks and the Internet;
- examined the effectiveness and efficiency of the continuous monitoring of the cyber assets that manage the (b) (7)(E) Dam; and
- determined whether additional security controls could bolster the (b) (7)(E) Dam's overall information technology (IT) security.

We conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

Office of Audits, Inspections, and Evaluations | Washington, DC

We found that the (b) (7)(E) Dam's (b) (7)(E) system was not air gapped, meaning it was not isolated from other nonessential networks. Such isolation insulates the system from USBR and DOI business networks, thus reducing the potential opportunity for internal and Internet-based threats to access the system.

We also found that the system did not have certain necessary safeguards to help ensure a strong security posture. These included: no automated safeguards in mobile media controls and enforcement; inadequate antivirus architecture; no vulnerability scanning; weak mitigation processes; inefficient continuous monitoring; no intrusion-detection capabilities; limited software support, and no memorandum of understanding (MOU) with externally connected entities.

We make 10 recommendations to strengthen the security posture of the (b) (7)(E) Dam's (b) (7)(E) system. Our recommendations, if implemented, should improve system security controls and prevent malicious activities.

Background

USBR manages five NCI-designated dams vital to the country's security, economy, and public health and safety. As one of the five, (b) (7)(E) Dam uses a (b) (7)(E) to manage water delivery and energy production. The system requires servers, workstations, switches, and cables, much like any computing arena, except that it is not intended for Internet connection. The system controls and monitors thousands of devices ranging from simple temperature sensors to automated controls for generators and gate functions. Each generator at the (b) (7)(E) facility alone uses approximately 250 sensors.

```
(b) (7)(E) Dam also is the key component of the (b) (7)(E) , a USBR project with multiple locations and facilities that provides hydroelectric power, flood control, and water storage for the upper (b) (7)(E) basin. The (b) (7)(E) (b) (7)(E) overall (b) (7)(E) performs operations support and is managed from (b) (7)(E) Dam. This support includes monitoring, power generation, and water management at several other facilities, including (b) (7)(E) (b) (7)(E) , and (b) (7)(E)
```

Critical infrastructure and cyber systems increasingly rely on IT for essential operations, making the protection of infrastructure from cyber threats a top priority. In the past, information about the cyber element of critical infrastructure was not widely known and thus helped protect the infrastructure. This anonymity is disappearing, however, as Internet connectivity increases throughout the United States and the globe. Recent DHS warnings indicate an increased threat to the (b) (7)(E)—operating NCI facilities.

Results of Inspection

The primary focus of this inspection was minimizing exposure for the (b) (7)(E) to various network vulnerabilities and threats. We found that the system included an unapproved connection to USBR's primary network infrastructure, widely expanding the threat footprint for the (b) (7)(E). Multiple additional control areas reviewed by OIG resulted in further findings of potential vulnerabilities and threats listed below.

Network Connectivity

Like other (b) (7)(E) managed by USBR, the (b) (7)(E) communicates among its various facilities through, among other things, the use of separate backup network connection mediums such as microwave, fiberoptic, and serial connections. The (b) (7)(E) is also connected to the (b) (7)(E) , which provides marketing and power reseller services for the energy generated by the (b) (7)(E) . The connection to the (b) (7)(E) allows (b) (7)(E) to request additional power generation based on client needs.

We discovered one unapproved connection to USBR's administration network, the

(b) (7)(E)

This connection provides the same operatoraccess capabilities to users across USBR without requiring a physical presence at the local
facility. This method of access bypasses specific logical and physical controls implemented at
the (b) (7)(E) facilities. Opening up access in this, and potentially other ways, also increases the
threat level, offering additional network entry points and opportunity to compromise the system.

Mobile Media Technical Safeguards

Although (b) (7)(E) Dam has developed procedures to allow mobile media use (e.g., smart phones, smart pads, flash drives, optical discs, and portable hard drives), no technical enforcement controls have been put in place to minimize threats. The (b) (7)(E) supports nine facilities in addition to (b) (7)(E). These sites are not equally staffed, allowing the absence of mobile media safeguards to create opportunities for unnoticed introduction of malware to the system.

The discovery of active malware such as the Stuxnet worm that attacked an industrial control system in Iran has heightened concern for malicious code that can damage (b) (7)(E). Stuxnet was originally designed to spread across systems using removable media, and is believed to have been introduced to the Iranian plant through a flash drive. Two other worms, Duqu and Flame, have been discovered that make use of the code found in Stuxnet, solidifying the need for strong mobile media controls.

Software Support

The (b) (7)(E) uses various software products to complete its mission. Four of the major commercial-off-the-shelf products used by this system have reached end-of-life status and no longer have vendor support:

(b) (7) (E) extended support ended in 2012
(b) (7) (E) support ended in 2003
(b) (7) (E) extended support ended in 2010
(b) (7) (E) support ended in 2003

Absence of vendor support means that these products will not be updated with security patches, leaving vulnerabilities unresolved and unreported.

Antivirus Architecture

The current (b) (7)(E) antivirus solution is missing three key features. First, it is a mix of open source solutions based on the (b) (7)(E) and does not have official vendor support available. Second, the antivirus solution does not provide a centralized reporting and alerting option to inform staff when the system has either taken action or discovered the need to take action against suspected files. Third, there is no centralized management console that allows staff to report on client status, modify configurations, or push engine and definition updates. These features are readily available in different antivirus platforms, and allow for more efficient, automated protection from malicious code.

Memorandum of Understanding

The system currently maintains an external connection to (b) (7)(E) that allows the system to monitor generation and request changes, but does not have in place an agreed-upon set of minimal security efforts and standards. Without this, the system's connection to an external source must be viewed as an open threat. USBR has spent several years focusing on this concern, trading draft MOU documents with (b) (7)(E) for consideration. To this date, no agreement has been reached. Due to recent organizational realignments in (b) (7)(E) connections are now managed only through its (b) (7)(E), instead of also involving the (b) (7)(E).

Continuous Monitoring

We found that the **(b) (7)(E)** does not have a fully automated continuous monitoring platform, required by the Federal Information Security Management Act of 2002 and National Institute of Standards and Technology Special Publication (SP) 800-37. Although the system has centralized audit log storage capabilities, it does not have an automated log reduction and alerting solution. Without this additional event processing, log review depends on staff availability to regularly review thousands of audit events daily. This is not possible without automated event filtering or a dedicated log review team. This situation creates the possibility of events going unnoticed for a lengthy period. The current auditing solution is a logging platform that can only support investigation and troubleshooting once an event is noticed. It does not provide the real-time monitoring necessary for notification of potentially problematic or security-related events.

(b) (7)(E) used a "Weakness Completion Verification Form" (WCVF) to validate that
it had fixed system weaknesses identified in its (b) (7)(E)
(b) (7)(E) . The OIG has found that the implemented solution does not meet the requirements
necessary to close the referenced POA&M.

Intrusion Detection System

An intrusion detection system – a key tool for information system monitoring, including real time analysis and reporting of network traffic – is not currently implemented to protect the (b) (7)(E). Without this monitoring tool, (b) (7)(E) staff cannot recognize and react to ongoing active incidents before these incidents impact service or operations capabilities.

This concern is magnified when coupled with previous findings that identified no MOUs covering external connections, as well as no near-real-time audit log event analysis and reporting. These three findings demonstrate an extended overall lack of awareness regarding present-state processing of activities and threats.

Vulnerability Scanning

The **(b) (7)(E)** does not currently undergo periodic vulnerability scanning as required by DOI. Staff at the local level has implemented a process that performs Nmap scans across the network, and Netstat checks on local systems. Nmap scans search for responding ports associated with differing services on **(b) (7)(E)**. These scans may include service and host identification techniques, beyond basic port identification. Netstat checks, which are host-based tests that report on local services and network connections, are also periodically conducted. These tools are useful when combined since each has capabilities the other does not, although they have the same primary focus of identifying services offered by a device.

Although these tools are an excellent addition to a security program and can be used to report on the status of services, they do not fulfill the requirement to perform periodic vulnerability scans. They also cannot be used to detect system vulnerabilities. Basic service scanning techniques do not include the capability to discover vulnerabilities within a service provided by the target host. Without adequate vulnerability scanning, using up-to-date vulnerability definitions, service scan reports will not identify weaknesses that could be manipulated.

Repeated Findings

Since these concerns are several years old, we believe they indicate a lack of movement toward weakness remediation. Some of these concerns, indeed, have been inaccurately described by USBR as being resolved through the use of a WCVF. One or more breakdowns appear to exist in the (b) (7)(E) vulnerability resolution process, leaving many findings open for exploitation much longer than necessary.

Recommendations

We make 10 recommendations based upon our findings.

- Disable the connection between (b) (7)(E)
- 2. Implement automated enforcement and monitoring of required mobile media security controls.
- 3. Update all software to supported versions and ensure a transition process is in place that is capable of maintaining vendor support levels.
- Deploy a centrally managed and reporting antivirus product that includes vendor support.
- 5. Complete an MOU between the (b) (7)(E)
 that includes a base security standard.
- 6. Deploy an automated log reduction and reporting tool for streamlined analysis and faster response.
- 7. Deploy an intrusion detection system that can perform real-time analysis of data traffic and incident alerting.
- 8. Begin performing periodic vulnerability scans.
- 9. Perform a review of the current findings' tracking and resolution process.
- 10. Review previously closed findings for accuracy and acceptable resolution methods.

Please provide us with your written response to this report within 30 days. The response should provide information on actions taken or planned to address the recommendations, as well as target dates and title(s) of the official(s) responsible for implementation. Please send your response to:

Donald W. Cairns
Deputy Assistant Inspector General
Office of Audits, Inspections, and Evaluations
U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428
1849 C Street, NW.
Washington, DC 20240

If you have any questions regarding this report, please contact me at 202-208-5745 or Theodore Dykstra at 303-236-9243.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



For Official Use Only, Not For Public Distribution
This report is exempt from disclosure under the
Freedom of Information Act, 5 U.S.C. § 552(b)(7)(f).

Report No.: ISD-IS-BOR-0003-2013



APR 1 0 2014

Memorandum

To:

Lowell D. Pimley

Acting Commissioner, Bureau of Reclamation

From:

Kimberly Elmore Kumberly Elmore Assistant Inspector General for Audits, Inspections, and Evaluations

Subject:

Inspection Report – IT Security of the (b) (7)(E)

Report No. ISD-IS-BOR-0003-2013

(b) (7)(E) Dam is one of five Bureau of Reclamation (USBR) dams, which were identified as National Critical Infrastructure (NCI) and which require special security considerations as documented by the Department of Homeland Security (DHS). (b) (7)(E) Dam provides operational support for the (b) (7)(E) and (b) (7)(E)also uses a (b) (7)(E)to automate, manage, and protect numerous processes, functions, and operations.

We completed an inspection of the (b) (7)(E)Dam (b) (7)(E) . Our objective was to assess the Bureau of Reclamation's (USBR) security posture for the (b) (7)(E) managed from the (b) (7)(E) Dam facility. To accomplish this b) (7)(E) objective, we-

- obtained a general understanding of (b) (7)(E) programs managed by USBR;
- Dam and interviewed officials from numerous programs in visited the (b)(7)(E)the dam's operations;
- reviewed documentation and internal reports provided by USBR staff;
- ascertained if the (b) (7)(E) network infrastructure was isolated from other U.S. Department of the Interior (DOI) business networks and the Internet;
- examined the effectiveness and efficiency of the continuous monitoring of the cyber assets that manage the (b) (7)(E) Dam; and
- determined whether additional security controls could bolster the (b) (7)(E) Dam's overall information technology security.

We conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

Office of Audits, Inspections, and Evaluations | Washington, DC

Freedom of Information Act, 5 U.S.C. § 552(b)(7)(f).

We found that the (b) (7)(E) Dam's (b) (7)(E) system was air gapped, meaning it was isolated from other nonessential networks. Such isolation insulates the system from USBR and DOI business networks, thus reducing the potential for internal and Internet-based threats.

We also found that the system did not have certain necessary safeguards to help ensure a strong security posture. The system has no automated safeguards in mobile media controls and enforcement and intrusion detection capabilities.

We make two recommendations to strengthen the security posture of the (b) (7)(E) Dam's (b) (7)(E) system. Our recommendations, if implemented, should improve system security controls and prevent malicious activities.

Background

USBR manages five NCI-designated dams vital to the country's national security, economy, and public health and safety. As one of the five, (b) (7)(E) Dam uses a (b) (7)(E) to manage water delivery and energy production. The system requires servers, workstations, switches, and cables, much like any computing arena, except that it is not intended for Internet connection. The system controls and monitors thousands of devices ranging from simple temperature sensors to automated controls for generator and gate functions. More than 20,000 sensors monitor events and operations management at multiple switchyards, powerhouses, the pumping plant, and system maintenance shop. The (b) (7)(E) also provides operational support for the (b) (7)(E) and (b) (7)(E)

Critical infrastructure and cyber systems increasingly rely on IT for essential operations, making the protection of infrastructure from cyber threats a top priority. In the past, information about the cyber element of critical infrastructure was not widely known and thus helped protect the infrastructure. This anonymity is disappearing, however, as Internet connectivity increases throughout the United States and the globe. Recent DHS warnings indicate an increased threat to the (b) (7)(E) operating NCI facilities.

Results of Inspection

Minimizing network exposure for the (b) (7)(E) was our primary focus. We found that the system was neither directly connected to the Internet, nor to DOI's or USBR's business networks. The connections that we did find had been documented with interconnection security agreements and network diagrams. We found, however, some control areas that could present risks to the system.

(b) (7)(E) *Upgrade*

(b) (7)(E) currently operates two (b) (7)(E) as part of a technology upgrade. The (b) (7)(E) system includes outdated hardware and software components, while the new

(b) (7)(E) system, developed in cooperation with the U.S. Army Corps of Engineers, uses more advanced technologies and processes. This new system has been implemented up to the point where all operator functions are performed through it, thus isolating the (b) (7)(E) components from direct access. All system communications are now filtered through (b) (7)(E) prior to reaching or leaving (b) (7)(E).

This arrangement has diminished threats to inherent system weaknesses that would require direct access for exploitation. Component failures still could create operational risks, however, mostly due to delays that impact project completion timelines. Staffing constraints imposed by the U.S. Army Corps of Engineers have extended the (b) (7)(E) completion goal to fiscal year 2016, which has slowed full installation of this critical technology.

Mobile Media Safeguards

The (b) (7)(E) Dam has developed manual procedures to manage mobile media devices (e.g., smart phones, smart pads, thumb drives, optical discs, and portable hard drives) for administrative IT functions. This includes centralized storage and periodic device inventory processes that help to minimize threats from unapproved devices. At this time, however, no technical enforcement controls have been put in place. The absence of mobile media safeguards creates opportunities for the unnoticed introduction of malware to the system.

The discovery of active malware such as the Stuxnet worm that attacked an industrial control system in Iran has heightened concern for malicious code that can damage systems. Stuxnet was originally designed to spread across systems using removable media, and is believed to have been introduced to the Iranian plant through a flash drive. Two other worms, Duqu and Flame, have been discovered that make use of the code found in Stuxnet, solidifying the need for strong mobile media controls.

Intrusion Detection System

An intrusion detection system – a key tool for information system monitoring, including real time analysis and reporting of network traffic – is not currently implemented to protect the (b) (7)(E) Without this monitoring tool, (b) (7)(E) staff cannot recognize and react to ongoing active incidents before these incidents have an impact on service or operations capabilities.

The (b) (7)(E) Dam staff recognizes this concern; however, edge network testing and deployment of an intrusion detection system has been halted due to bandwidth resource requirements. Any products purchased to meet this need are not yet fully operational and would need enhancement.

Recommendations

We make two recommendations based upon our findings:

- 1. Implement automated enforcement and monitoring of required mobile media security controls.
- 2. Deploy an intrusion detection system that can perform real-time analysis of data traffic and incident alerting.

Please provide us with your written response to this report within 30 days. The response should provide information on actions taken or planned to address the recommendations, as well as target dates and title(s) of the official(s) responsible for implementation. Please send your response to:

Donald W. Cairns
Deputy Assistant Inspector General
Office of Audits, Inspections, and Evaluations
U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428
1849 C Street, NW.
Washington, DC 20240

If you have any questions regarding this report, please contact me at 202-208-5745 or Theodore Dykstra at 303-236-9243.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

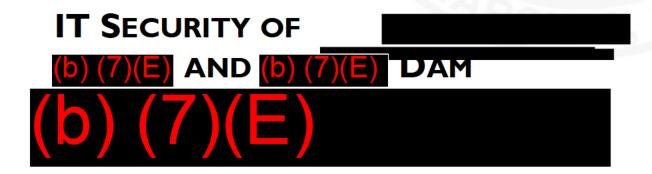
By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240





For Official Use Only, Not For Public Distribution
This report is exempt from disclosure under the
Freedom of Information Act, 5 U.S.C. § 552(b)(7)(f).

Report No.: ISD-IS-BOR-0002-2013



APR 1 0 2014

Memorandum

To:

Lowell D. Pimley

Acting Commissioner, Bureau of Reclamation

From:

Kimberly Elmore Kimberly Elmore

Assistant Inspector General for Audits, Inspections, and Evaluations

Subject:

Inspection Report – IT Security of the (b) (7)(E) and (b) (7)(E) Dams

(b) (7)(E)

Report No. ISD-IS-BOR-0002-2013

(b) (7)(E) and (b) (7)(E) Dams are two of five Bureau of Reclamation (USBR) dams which were identified as National Critical Infrastructure (NCI) and which require special security considerations as documented by the Department of Homeland Security (DHS). (b) (7)(E) Dams use a (b) (7)(E) to automate, manage, and protect numerous processes, functions, and operations.

We completed an inspection of (b) (7)(E) and (b) (7)(E) Dams' (b) (7)(E). Our objective was to assess the USBR' security posture for the (b) (7)(E) and (b) (7)(E) Dams (b) (7)(E), which is managed from the (b) (7)(E) in (b) (7)(E) To accomplish this objective, we—

- obtained a general understanding of (b) (7)(E) programs managed by USBR;
- visited the (b) (7)(E) Dam, (b) (7)(E) Dam, and (b) (7)(E) in (b) (7)(E) and interviewed officials from numerous programs in the dams' operations;
- reviewed documentation and internal reports provided by USBR staff:
- ascertained whether the (b) (7)(E) network infrastructure was isolated from other U.S. Department of the Interior (DOI) business networks and the Internet;
- examined the effectiveness and efficiency of the continuous monitoring of the cyber assets that manage the (b) (7)(E) and (b) (7)(E) Dams; and
- determined whether additional security controls could bolster the (b) (7)(E) and (b) (7)(E) Dams' overall information technology security.

We conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

Office of Audits, Inspections, and Evaluations | Washington, DC

We found that the (b) (7)(E) and (b) (7)(E) Dams' (b) (7)(E) system, known as the (b) (7)(E) was air gapped, meaning it was isolated from other nonessential networks. Such isolation insulates the system from USBR and DOI business networks, thus reducing the potential for internal and Internet-based threats.

We also found that the system had necessary safeguards to help ensure a strong security posture. The system had implemented automated safeguards in mobile media controls and enforcement and integrated continuous monitoring capabilities. At this time, we have no recommendations for system-level control improvement for the (b) (7)(E)

Background

USBR manages five NCI-designated dams vital to the country's national security, economy, and public health and safety. As two of the five, of the five, and of the five, of th

providing operational support for other water management sites in addition to the providing Dams. The (b) (7)(E) network includes more than 25,000 data points used for monitoring events and operations management at multiple switchyards, powerhouses, pumping plants, and control centers.

Critical infrastructure and cyber systems increasingly rely on IT for essential operations, making the protection of infrastructure from cyber threats a top priority. In the past, information about the cyber element of critical infrastructure was not widely known and thus helped protect the infrastructure. This anonymity is disappearing, however, as Internet connectivity increases throughout the United States and the globe. Recent DHS warnings indicate an increased threat to the (b) (7)(E)

Results of Inspection

Minimizing network exposure for the (b) (7)(E) was our primary focus. We found that the system was neither directly connected to the Internet, nor to DOI's or USBR's business networks. The connections that we did find had been documented with interconnection security agreements and network diagrams. Within this focus, we did not have any negative findings regarding (b) (7)(E) We did encounter several practices that we felt USBR staff had implemented with efficiency and effectiveness.

Documentation

We found that the documentation we reviewed appeared consistently thorough and detailed. Specific documentation was available, and everything provided to us met the

For Official Use Only, Not For Public Distribution

objectives of this inspection. This documentation included components, policies and procedures, technical details, and architectural descriptions related to the (b) (7)(E) (b) (7)(E)

Monitoring

The (b) (7)(E) team has implemented a detailed continuous monitoring solution. The chosen platform performs central log reduction and systemwide device reporting. The (b) (7)(E) solution allows for collecting logs from multiple vendor products and providing a single interface for event review to assist with incident correlation and analysis.

In addition to the central log management solution, a Universal Serial Bus (USB) device monitoring system that reports into the continuous monitoring platform, has been implemented across (b) (7)(E) This system monitors and reports all USB activities, including insertion of removable media and devices (e.g., smartphones, flash drives, and external hard disk drives) to system servers and clients. The (b) (7)(E) team noted that the USB monitoring product they chose is capable of defining specifically permitted or prohibited devices so that their insertion would be centrally reported and the system would have the capability to allow or block their use. The staff at the (b) (7)(E) is currently investigating options for implementing this feature.

Please send any written response you might have to:

Donald W. Cairns
Deputy Assistant Inspector General
Office of Audits, Inspections, and Evaluations
U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428
1849 C Street, NW.
Washington, DC 20240

If you have any questions regarding this report, please contact me at 202-208-5745 or Theodore Dykstra at 303-236-9243.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



EVALUATION OF THE ACTIVE DIRECTORY

Report No.: ISD-EV-MOA-0006-2010



Memorandum

AUG 17 2010

To: Bernard J. Mazer

Chief Information Officer, Department of the Interior

From: Eddie Saffarinia

Assistant Inspector General for Information Technology

Subject: Final Report – Evaluation of the Active Directory

(Assignment Number ISD-EV-MOA-0006-2010)

We conducted a technical evaluation of the implementation for the DOI Active Directory to assess the efficiency and effectiveness of its information security controls solutions. The evaluation was conducted at the Enterprise Infrastructure Division in Lakewood, CO, and we interviewed all bureaus and offices designated as Active Directory points of contact.

We concluded that security and monitoring investments are not being fully used. We found no Department-wide standardization and, in some cases, none within bureaus. An inadequate separation of duties exists for system administrators within the Department's Enterprise Infrastructure Division. We determined that continuous monitoring has not been consistently integrated throughout bureaus and offices. Furthermore, various Active Directory functions have been duplicated throughout the Department, bureaus, and offices.

We made four recommendations to address the issues identified in the report. We ask that the Department apprise us within 30 days of the date of this memorandum of the actions it takes or plans to take in response to this report. If you have any questions regarding the report, please call me at (703) 487-5369. Staff may contact Matthew Bunko at (303) 236-9152.

cc: Deputy Assistant Secretary, Technology, Information, and Business Services Chief Information Security Officer, Department of the Interior Audit Liaison Officer, Department of the Interior

Table of Contents

Results in Brief	1
Introduction	2
Objective	2
Background	2
Management and Administration	4
Labor Cost and Number of Personnel	8
Ascertain of Uniqueness of Requirements	9
Applications that Use AD for Authentication	10
Architecture	11
Duplicative Functions	11
IT Security Controls	15
Separation of Duties	15
Least Privilege	15
Continuous Monitoring	16
Conclusion and Recommendations	19
Conclusion	19
Recommendation Summary	19
Appendix 1: Objective, Scope, Methodology, and Related Coverage	20
Appendix 2: Acronyms and Other Reference Terms	22

Results in Brief

We found that the Department's Active Directory is constructed along organizational boundaries rather than technological boundaries as is recommended by the manufacturer and by common best practices. Common geographic areas had multiple pieces of equipment that were logically separated from each other. This strategy is not cost efficient, as more equipment is required to serve offices in the same geographic area and hinders communication and file sharing for users who are co-located or working on common tasks. By reorganizing AD along technology boundaries, the Department could reduce the amount of equipment needed and improve collaboration amongst end users.

We found that the investments for enhancing Active Directory information security are underused, and as a result, impairs the Department's capability to perform oversight. We determined that only 34 percent of the bureau and office servers connect to the Department's security information and event management infrastructure, and none connect to the Department's System Center Configuration Manager infrastructure, which provides critical information such as asset intelligence and critical patch status, and which also deploys patches.

We also found the Department has not accomplished its goal to achieve Active Directory operational standardization, as outlined in Title III of the E-Government Act, titled the Federal Information Security Management Act (FISMA), which emphasizes the need for organizations to develop, document, and implement an organization-wide information security program that identifies, mitigates, and monitors information and information system risks.

On March 1, 2010, after this evaluation was conducted, the Department of the Interior Information Technology Innovation and Efficiencies Team was created. It initiated a risk-based Information Security Services project to promote more efficient and cost-effective information security methods across the Department. In addition, this team will identify better IT services with fewer resources and establish savings through innovation.

Introduction

Keeping track of and monitoring IT resources on the network is a time-consuming task. Even on small networks, users tend to have difficulty sharing information and finding network file and printer shares. A network directory establishes a logical structure for managing the environment. Without some kind of network directory, medium and large networks are impossible to manage, navigate, and collaborate.

Objective

Our objective was to determine whether DOI had implemented effective security controls on its Active Directory domains (a consolidation of IT resources logically grouped and which share a central directory). In addition, we reviewed DOI's compliance with:

- its own strategic plans,
- industry best practice,
- FISMA,
- National Institute of Standards and Technology's Special Publication 800-53, which provides guidance and recommendations for implementing IT security controls for Federal information systems, and
- the Department's IT Security Policy Handbook, which requires bureaus and offices to implement IT Security controls in accordance with SP 800-53 guidance.

Background

Microsoft's Active Directory (AD) is intended to simplify user and resource management while creating a scalable, secure, and manageable infrastructure for deploying additional important and emerging technologies. It includes the ability to record information about different objects. For example, Active Directory, stores information, much like a phone book, about user accounts, such as names, passwords, phone numbers, etc., and enables other authorized users on the same network to access this information.

Active Directory provides security in the following major areas:

- Access: Active Directory requires a user to establish an account to log onto a computer. The account creates the user's identity and then the operating system uses it to authenticate him or her and grant authorization for accessing specific domain resources;
- Permissions: Active Directory confirms the identity of any user logging onto a domain and lets them access resources such as data, applications, or

¹ Microsoft's TechNet provides access to technical question and answers for implementation and best practices (http://technet microsoft.com/en-us).

printers located anywhere on the network. A key feature is its single signon capability, which makes multiple applications and services available to the user over the network without having to provide credentials more than once;

- Rights: Active Directory secures resources from unauthorized access.
 After a user account receives authentication and can potentially access resources, how much access gets granted is determined by what rights are assigned to the user and which permissions are attached to the resources being accessed; and
- Organization: Active Directory organizes computing resources and makes them available to authorized users, provides Administrators with the tools and access necessary to efficiently manage interconnected computing resources, and establishes a scalable and flexible framework from which new technologies can be interconnected.

In August 2002, the DOI Information Technology Management Council directed that planning be initiated for the unified deployment of an Active Directory as the Department's enterprise directory service. The Management Council agreed that the target architecture would be based on a single enterprise forest, containing one domain per bureau and office, and providing organizational and administrative system boundaries.²

The Department's Information Technology Strategic Plan FY 2007 through 2012, September 2006 ("Plan") described Active Directory as providing a "single authoritative user directory for controlling access to IT systems and services." The Plan stated four strategic objectives for AD of which we only found two of them to be partially implemented:

- Consolidate Domain Name Services for the Enterprise Services Network;
- Migrate all bureaus to the Enterprise AD;
- Fully implement the standards for AD; and
- Migrate all AD domain controllers to Enterprise Management.

In 2008, the Department hired an outside expert to review its Active Directory implementation. The Department's own expert concluded, "Configuring DOI as a single forest with a single domain follows Microsoft and industry best practice, standardizing operations and addressing the PoA&Ms [Plan of Action and Milestones], but it does not meet DOI's strategic and political objectives."

_

² Information Technology Enterprise Active Directory Project, July 13, 2004.

Management and Administration

The fragmented approach to AD management is inefficient and is not producing satisfactory results. The Department Chief Information Officer directed that governance and a configuration management board be established in a July 13, 2004 signed memorandum, "Information Technology Enterprise Active Directory Project." The associated tasks were to be completed by August 2004, yet, more than four years later, the DOI Change and Configuration Management Handbook, version 1.0, October 1, 2008 (CCM Handbook) states that the governance structure was submitted to the Management Council in July 2008 and gained final approval in October 2008.

Active Directory is intended to be flexible in order to rapidly accommodate a dynamic environment, but the Department's Change and Configuration Management process is complex. As a result, implementing changes is cumbersome and slow.

The CCM Handbook included a diagram to illustrate the CCM process (Figure 1), which it stated was sanctioned during its April 17, 2008 meeting after having reviewed industry best practices.

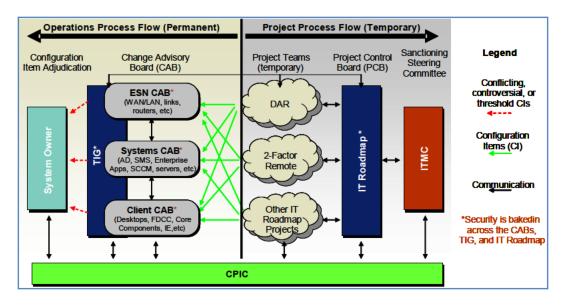


Figure 1. CCM process. Image source: Department of the Interior.

A contractor hired by the Department concluded in October 2008 that the Department's Active Directory configuration was not aligned with industry best practices.

In 2008, the Department's E-Government (E-Gov) initiative contained six elements for bureaus to complete within the Enterprise Active Directory arena to

eliminate redundancy and inefficiency and improve standardization across the agency. The following three of the six elements have not been fully implemented:

- Auditing and Logging (Function 3): Enterprise Active Directory Operations Standardization Implement enterprise level logging service that centrally aggregates, correlates, stores, and provides appropriate access to all domain controller log files (by March 20, 2009);
- Security Event Management (Function 4): EAD Operations Standardization – Implement Security Event Management as prescribed in the Enterprise Active Directory Project Plan (by June 30, 2009); and
- Domain Controller Security Technical Information Guideline Baseline Monitoring and Compliance (Function 5): Enterprise Active Directory Operations Standardization – Integrate with asset inventory auditing and logging solution, definitions, standardizations, and baselines from other functions as prescribed in the Enterprise Active Directory Project Plan (by October 30, 2009).

Department level oversight has been inadequate for the remaining three elements which have been implemented. This became apparent when we requested information that should have been easily created and provided if the bureaus and offices were in compliance with the Departmental requirements in the E-Gov initiative. Table 1 demonstrates the bureaus' failure to progress in the E-Gov initiative and the Department's failure to oversee and obtain compliance from all bureaus and offices

Questions Asked to the Department

	Bureau/ Office	ō	MMS	ZPS	SC	JSGS	DHTA	VBC	3IA	MSC	ОНА	3LM	3OR	FWS	SOL
SUUM	Compliance report on approved configurations for Domain Controllers														
	Provide patch status for Critical patch (KB978207)														
	Adobe Products														
	Provide list of free disk space on Domain Controllers														
	Provide status report for last three patches pushed														
	Users accounts created manually after Jan. 15, 2010														
N E T	Users added to or removed from Domain Admin Group in January 2010														
- Q	Security Event log cleaned in January 2010														
	User logon failed due to time restrictions in January 2010														
Leg	end: 100 percent		Par	tial			0 Pe	rcen	t [

Table 1.

The table illustrates that none of the bureaus are connected to System Center Configuration Manager, in which the Department invested more than \$500,000 so it could gain insight into bureau IT infrastructure, hardware, and software assets, Configuration Management and compliance with mandatory computer configurations, and reporting capabilities on critical patches.

Likewise, the table also illustrates that less than 35 percent of the bureaus and offices servers were connected to NetIQ Security Manager, a security information and event management infrastructure, in which the Department invested \$400,000 with the purpose of giving it a centralized enterprise level logging and auditing capability, real-time alerting capability to key Departmental personnel on key events, and group policy auditing and reporting.

If Department bureaus were in full compliance with these elements, the Department would have access to key information, such as critical patch status, real-time alerts, asset inventory, computer baseline deviations, configuration management, and the creation of unauthorized accounts, which would allow the Department to perform proper oversight.

Bureaus' lack of compliance with the DOI Enterprise Active Directory Operations Standardization guidance inhibits the Department's ability to move forward with oversight, compliance, and standardization. On December 1, 2009, the Department Chief Information Officer signed memorandum "DOI Access Procedures for Bureau/Office Active Directory and Email Systems," in which he established procedures to be implemented by January 15, 2010, to include:

- Creating all Active Directory accounts for new employees and new contractors with the DOI Access System³; and
- Deploying NetIQ Security manager agents on bureau domain controllers (per 2008 E-Gov Scorecard: Enterprise Infrastructure, Element 5.3) is required to enable monitoring of user account creation. All bureau domain controllers must meet the scorecard requirements.

We found no compliance with the requirement to create new Active Directory accounts through the DOI Access System, and found that FWS, BLM, and BOR created user accounts after the January 15, 2010 deadline. Furthermore, we were unable to determine compliance for BIA, MMS, NPS, OS, NBC, OHTA, and USGS because the Department was unable to provide a report.

The NetIQ Security Manager, an enterprise tool for monitoring IT systems and security management, was not implemented on 66 percent of the domain controllers⁴ at BIA, MMS, NBC, NPS, OHTA, OS, and USGS. (Domain

³ The DOI Access System was created to integrate with existing authoritative data sources to establish required identity data for sponsoring employees and contractors for Access cards with valid Active Directory credentials.

⁴ A domain controller is a server that runs a version of Microsoft's server 2000, 2003, or 2008 and has the Active Directory Service installed.

controllers perform significant roles such as authentication requests [i.e., logging in, checking permissions for access to resources] and security and event logging of essential events.) NetIQ requirements have been fulfilled for 34 percent of the domain controllers at BLM, BOR, FWS, OHA, OSM, OST, and SOL.

Labor Cost and Number of Personnel

The fragmented environment impacts the resources required to manage Active Directory.

We requested the Department provide a list of personnel with significant Active Directory duties, costs associated with labor, and the percentage of time performing these duties. We determined that labor associated with managing Active Directory is just under \$9 million annually (Figure 2).

Labor Dollars spent on personnel with Significant AD responsibilities

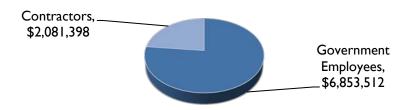


Figure 2. Numbers pulled from the 2010 annual rates by grade and step. Contract dollar amounts provided by bureaus. Dollar amount adjusted for overall percentage of Active Directory duties reported.

This is the breakdown of Government and contractor personnel:

- Of the personnel identified with significant Active Directory duties,
- did not know the percentage of time spent on Active Directory administration.
- were Government employees, and
- were contractors.
- Of the personnel identified, were domain administrators at bureaus (Figure 3). (Domain administrators have complete administrative rights to their specific domain.) were identified as enterprise administrators at the Departmental level. (Enterprise administrators have complete administrative rights over the DOI enterprise.)
- Government employees and contractors with significant Active Directory duties spent an average of 30 and 28 percent, respectively, on Active Directory administration.

Personnel designated as Domain or Enterprise Administrators

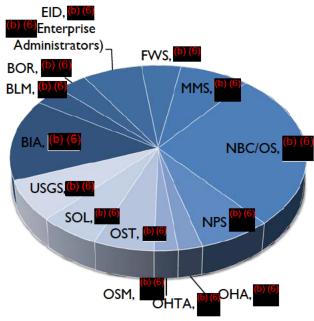


Figure 3. Administrators.

Ascertain the Uniqueness of Requirements

Since best practice is to deploy Active Directory consistently across the environment, and the Department's Active Directory is dispersed throughout each individual bureau, we interviewed key bureau personnel to establish the level of uniqueness throughout the DOI environment.

We found OST, SOL, OHTA, OHA, MMS, BIA, BLM, and BOR had no uniqueness concerns.

The following bureaus brought up these uniqueness concerns:

- FWS: "Regions within FWS can say 'no' to mandates," and group policies are not getting out due to network bandwidth issues;
- USGS: Architected for 79 domain controllers to ensure functionality in the offices if network connectivity is lost;
- NPS: "We have a distributed environment and have challenges getting users connected;" and
- NBC and OS: Efforts standardizing across NBC.

Applications that Use AD for Authentication

When interviewing bureaus and offices, we asked what percentage of their applications use Active Directory for authentication. We found various degrees of implementation. The technical staff of the following bureaus gave these estimates and statements for the number of its applications that use Active Directory for authentication:

- SOL and OHTA: 100 percent;
- NPS: 40 percent;
- BOR:10 percent;
- FWS: 70 to 80 percent of its major applications;
- BIA: 25 percent of its applications use Active Directory;
- OST: 90-plus percent;
- BLM: 75 percent of the major applications;
- NBC and OS: No percentage reported ("The majority of the applications at NBC are not Active Directory authenticated");
- MMS: Three major applications ("Do not know how some applications authenticate");
- USGS: No percentage reported (Lotus is the authoritative directory, but trying to move to Active Directory as the authoritative directory. Does not track science-related applications to see if they use Active Directory for authentication);
- OHA: No percentage reported (Some applications use Active Directory and others do not, but moving toward Active Directory for authenticating); and
- OSM: No percentage reported ("Major applications at OSM do not use Active Directory for authentication, but we plan to talk to vendors to change it").

Architecture

The Department's Active Directory group policy structure is duplicative and complex. We found a lack of consistency among bureaus that are connected to the Department. We determined bureaus and their respective regions, districts, sites, and science centers implemented various technical capabilities to monitor Active Directory resources and IT assets. The fragmented approach that has led to the Department having limited insight into its bureaus is inefficient and costly.

We requested that bureaus and offices identify domains⁵ in which they house IT resources. Nine bureaus and offices (BIA, BLM, BOR, NPS, OS, OSM, OST, SOL, and USGS) reported that they only have one domain with all IT resource incorporated. Five bureaus (FWS, MMS, NBC, OHA, and OHTA) reported that they have more domains than their primary domain. The five organizations have a combined 15 additional domains.

Duplicative Functions

We found servers throughout the bureaus that have the potential to be consolidated. Of the data provided, we chose seven cities and found numerous servers in the same city but from different bureaus (domain controllers and file, print, or member servers), as demonstrated in Figures 4 and 5. Moving away from the organizational boundaries could potentially lead to consolidating these types of servers and consequently to significant cost savings in hardware, software, and administration. We were unable to add the location of 269 servers within FWS because locations were not provided.

11

⁵ A consolidation of IT resources logically grouped which share a central directory.

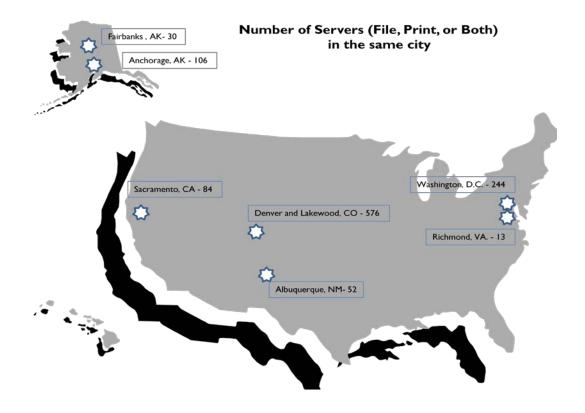


Figure 4.

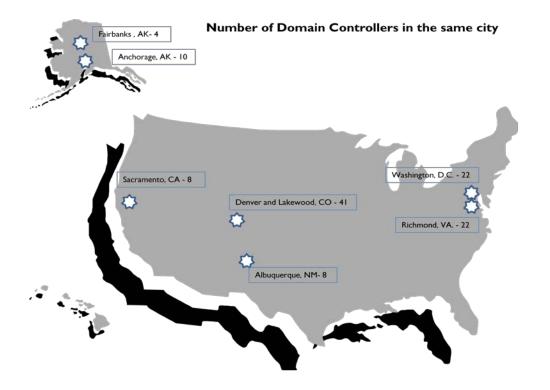


Figure 5.

Within the bureaus, we identified 4,460 servers, which serve users for printing or storing information, or both (Figure 6 shows them by bureau).



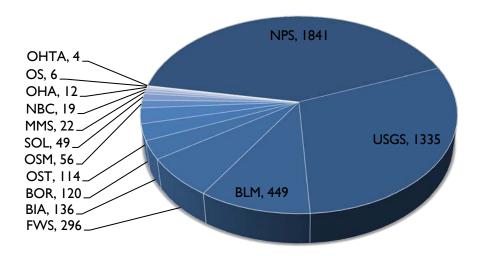


Figure 6. DOI has a total of 4,460 servers.

In reviewing the data provided by the bureaus and offices, we found 5,902 group policies⁶ and 3,978 organizational units⁷. We found that Active Directory policies are managed differently among and within bureaus, for example:

- BIA blocked inheritance of pertinent policy to its domain controller's organizational unit. The policy it blocked is essential to the security and configuration of its domain controllers;
- NPS duplicates group policies for each location, thus duplicating efforts and increasing the risk for errors. We also found conflicting policies regarding trusted sites applied to Internet Explorer. Conflicting policies increase the time it takes for a user to logon because the policies have to be run twice;
- OST blocked all policies to one organizational unit where workstations were nested. These workstations rely on policies being pushed down to be compliant with Federal Desktop Core Configurations as mandated by OMB M-08-22, Guidance on the Federal Desktop Core Configuration; and

⁶ Group Policies are a set of rules used to centrally manage and control user accounts and computers. Essentially it configures operating systems and controls what a user can and cannot do on a computer.

⁷ Organizational Units (OUs) are AD containers in which you can place users, groups, computers, and other OUs

⁸ Domain Controllers are servers which can have many functions in AD, but the most critical function is its ability to authenticate users.

• OS duplicated policies within their Office of the Chief Information Officer's Organizational Unit.

The benefits of aligning the Department under technical boundaries instead of organizational boundaries include better adaptability, maintainability, and functionality.

Number of Group Polices and Organizational Units per Bureau or Office

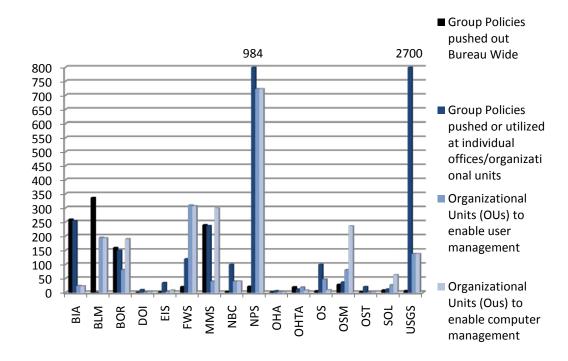


Figure 7. Complexity of policies and organizational units.

Recommendation

I. The Department re-architect Active Directory along technology boundaries rather than organizational boundaries.

IT Security Controls

The Department is responsible for continuously monitoring and controlling IT resources agency-wide, according to FISMA and The Guide for Applying the Risk Management Framework to Federal Systems, SP 800-37 Rev 1. Having the most complete, accurate, and reliable information on the security status of information systems is essential for agency officials.

We found the Department lacks a complete continuous monitoring program in Active Directory and did not have the critical security controls, such as separation of duties, least privilege, and configuration management necessary to appropriately manage Active Directory.

Separation of Duties

In FY2009, 677 employees and contractors were fully devoted to information security across the Department, yet not one was monitoring the administrators who have the highest level of administrative rights and full control of the DOI forest resources. When reviewing for separation of duties, we found enterprise administrators performing functions such as auditing security on one another. Without appropriate separation of duties the organization cannot be assured that user accounts do not have escalated privileges or that unauthorized accounts are not created.

Recommendation

2. The Department implements separation of duties for administrators.

Least Privilege

Implementing least privilege is ensuring that typical users' accounts are limited to only the amount of rights needed to do the job. The principle of least privilege is important in enhancing the protection of data and functionality within an environment.

We found the least privilege concept not being fully employed throughout the bureaus. We found domain administrators throughout the Department. NPS is the largest of the bureaus and it has domain administrators, whereas, the smaller bureaus, NBC and OS, have domain administrators.

When we reviewed the members of the OS domain administrators group, we found one person having both of his accounts (typical user and elevated privilege account) in the domain administrators group. This creates a serious security concern because the user always logs on with full privileges to the OS domain. This places the Department's information assets at risk any time the user accesses

the Internet. If a piece of malware on a Web page attempted to do harm, it would have domain administrative rights.

We reviewed specified training accounts within a number of bureaus and found there was no standard to lock down these generic accounts. We found logon hours allowed some accounts to logon on any day at any time and others to have the time and day restricted. We found that the bureaus did not always restrict where the training accounts could logon despite it being an option.

Continuous Monitoring

The Department cannot manage what it does not know. We conducted interviews and requested data to determine if security controls were monitored on an ongoing basis in accordance to FISMA and SP 800-37, Rev 1. We found components of a continuous monitoring program were established to monitor Active Directory and IT resources, but we determined they were not consistently applied throughout the bureaus.

We determined the Department invested in and implemented the capabilities to allow oversight into the bureaus' tools for monitoring Active Directory, but not all of them allow the Department to have insight (Figure 8). In fact, none of the bureaus allow the Department access to their asset inventory auditing and logging.

Percentage of bureaus that have migrated to the Department to allow oversight and monitoring

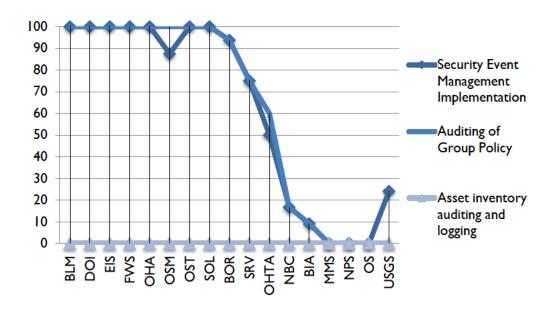


Figure 8. Compliance with oversight and monitoring.

Recommendation

3. Bureaus comply with Departmental policy and procedures to allow insight and oversight into all domains.

We found the Department did not monitor or audit the bureaus' user accounts. SP 800-53, revision 3 establishes guidelines for account management and identifying user accounts that are unused, have passwords that never expire, do not require a password, or do not require a password age. Not all bureaus were monitoring these attributes (Table 2), but we identified seven products used by bureaus for this auditing.

Not all bureaus had established a schedule to audit these attributes. We found inconsistency, with some bureaus performing audits ranging from monthly or quarterly to ad hoc or when time permitted.

Auditing of User Accounts

	BIA	BLM	BOR	DOI	EIS	FWS	MMS	NBC	NPS	OHA	OHTA	SO	OSM	OST	SOL	USGS
Does your bureau audit AD for unused accounts?																
Does your bureau audit AD for accounts with passwords that never expire?																
Does your bureau audit AD for accounts that do not require a pass-word?																
Does your bureau audit AD for account password age?																

Legend: Yes		No	
-------------	--	----	--

Table 2.

Recommendation

4. The Department establishes and document procedures for implementing, managing, and monitoring Active Directory.

Conclusion and Recommendations

Conclusion

To provide a secure and effective enterprise services within DOI, emphasis must be placed on standardization, separation of duties, and continuous monitoring. Already purchased security and monitoring investments must be used to the fullest extent and implemented consistently throughout the Department.

Recommendation Summary

To address the deficiencies identified in this report, we recommend:

- 1. The Department re-architect Active Directory along technology boundaries rather than organizational boundaries.
- 2. The Department implements separation of duties for administrators.
- 3. The Department establishes and document procedures for implementing, managing, and monitoring Active Directory.
- 4. Bureaus comply with Departmental policy and procedures to allow insight and oversight into all domains.

Appendix I: Scope, Methodology, and Related Coverage

The objective of our evaluation was to assess the Department's Active Directory to determine if:

- All Bureaus were migrated to the Enterprise Active Directory;
- The full implementation of standards for Active Directory was completed;
 and
- The migration of all Active Directory domain controllers to Enterprise Management was completed.

In addition, our objective was to determine if information security controls were implemented in accordance with legislation, policy, and standards, as well as to determine if those controls were efficient, effective, and operating as intended.

Our evaluation extended to all DOI bureaus using Active Directory.

Other OIG audits and evaluations related to the work performed during this evaluation include:

- "Computer Configuration Evaluation," Report No. ISD-EV-MOA-0003-2009, August 2009.
- We found widespread noncompliance with mandatory Federal Desktop Core Configuration standards and noncompliance with directives issued by the Department's Chief Information Officer.
- "Verification of FY 2007 IT Security Recommendations," Report No. ISD-EV-MOA-0002-2009, September 2009.
- We found management oversight of resolving the OIG information security recommendations absent and a recent investment to improve information security ("Cyber Security Assessment Management application") not fully leveraged.
- "FY 2009 Federal Information Security Management Act (Revised)," November 16, 2009.
- We found widespread noncompliance with legislation and policy.

We conducted our evaluation in accordance with the Quality Standards for Inspections as put forth by the Council of the Inspectors General on Integrity and Efficiency. We included tests of records and other procedures that we considered necessary under the circumstances. To accomplish our objective, we conducted the following activities:

• Reviewed applicable laws, regulations, Office of Management and Budget guidance, National Institute of Standards and Technology standards.

Government Accountability Office reports, and Department and bureau policies;

- Reviewed documentation and Active Directory implementation;
- Interviewed Department and bureau IT security personnel; and
- Performed onsite inspections of bureau locations.

Appendix 2: Acronyms and Other Reference Terms

AD Active Directory

BIA U.S. Bureau of Indian Affairs
BLM U.S. Bureau of Land Management
CCM Change and Configuration Management

DOI Department of the Interior

FISMA Federal Information Security Management Act

FWS U.S. Fish and Wildlife Service
IT Information Technology
NPS U.S. National Park Service

NPS U.S. National Park Service OIG Office of Inspector General

OMB Office of Management and Budget

OUs Organizational Units
OS Office of the Secretary

PoA&M Plan of Action and Milestones

SP Special Publication



INFORMATION SECURITY EVALUATION OF THE NATIONAL INTERAGENCY FIRE CENTER

Table of Contents

ACRONYMS AND OTHER REFERENCE TERMS	2
RESULTS IN BRIEF	3
INTRODUCTION	4
BACKGROUND	5
EVALUATION RESULTS	6
THE NETWORK	7
DATA CENTER	9
WIRELESS NETWORKING	
TECHNICAL CONTROLS	10
ACCOUNT MANAGEMENT	10
NETWORK ACCESS CONTROL	11
VULNERABILITY SCANNING	
CONFIGURATION MANAGEMENT	12
INCIDENT DETECTION AND RESPONSE	14
NONCOMPLIANCE WITH GUIDANCE	15
RADIO SYSTEM	16
RECOMMENDATIONS	17
APPENDIX 1: OBJECTIVE, SCOPE, METHODOLOGY, AND RELATED COVERAGE	18

Acronyms and Other Reference Terms BIA......U.S. Bureau of Indian Affairs ESN Enterprise Services Network FDCCFederal Desktop Core Configuration FIPS Federal Information Processing Standards FISMA Federal Information Security Management Act FISSA......Federal Information System Security Awareness IG......Inspector General Information Security Division LMR.....Land Mobile Radio OMB Office of Management and Budget OSOffice of the Secretary PIA Privacy Impact Assessment USDA......U.S. Department of Agriculture(b) (7)(E)

Results in Brief

Information technology (IT) resources are an essential element of current wildland fire management and operations. All indications show that IT will continue to play a significant role in the future.

We found that the IT environment is complicated and difficult to manage because it is collocated and shares cabling but is technologically separated. This separation typically makes collaboration among end users difficult and expensive to maintain. An estimated 125 users require multiple computers on their desk in order to navigate the fragmented network that bridges the Department of Agriculture and the

Department of Interior. Moreover, the current network design combines routine administrative and personal network traffic with high priority network traffic that serves firefighting operations and management. Isolating high priority traffic from routine traffic is impractical due to the complex design of the network. We concluded that compliance with the myriad of individual bureau policies and standards impedes efficient and cost effective operations at the National Interagency Fire Center (NIFC) and puts firefighters and the public at higher risk of injury or death.

"Recent developments in internet communications and information organization will allow fire management to rethink mediums and opportunities for broader access and greater stakeholder and public engagement."

2009 Quadrennial Fire Review

NIFC uses Land Mobile Radios (LMR) for firefighting operations as well as for routine operations including security

and law enforcement on the NIFC campus in Boise, ID. We found that radios were not certified or accredited to operate.

We found that existing technology for securing user accounts was ineffective. We were not detected when we used a username and password that we found written on a piece of paper to access the BLM network. Access to this network allowed us to potentially obtain personally identifiable information.

Our evaluation found that NIFC generally complied with legislation and policy. There is opportunity, however, to improve operations at NIFC with little up-front costs. Our recommendations will lower costs, improve collaboration, enable NIFC to dedicate network resources to high priority mission tasks, and further enhance personnel and public safety.

Introduction

In support of their overlapping responsibilities for land management and conservation, DOI and USDA participate in the National Interagency Fire Center (NIFC), located in Boise, ID. NIFC is the nation's support center for wildland firefighting. NIFC is comprised of eight Agencies and organizations. The interagency cooperation concept makes decision making difficult because NIFC has no single director or manager. DOI has four bureaus represented at NIFC: Bureau of Land Management (BLM), Bureau of Indian Affairs (BIA), U.S. Fish and Wildlife Service (FWS), and National Park Service (NPS). USDA is represented at NIFC by the Forest Service.

The Quadrennial Fire Review is a strategic assessment process conducted every 4 years to evaluate existing mission strategies and capabilities against best estimates of future environment for fire management. This review is a joint effort of the five Federal natural resource management agencies and their State, local, and tribal partners that constitute the wildland fire community. The objective is to create an integrated strategic vision document for fire management.²

The 2009 Quadrennial Fire Review found that information technology for electronic status, location, tracking, and ordering are essential for timely resource coordination and concluded that new technologies, particularly in remote sensing and communications, will minimize direct human participation in high risk activities and reduce risk related to fire management operations.

"Implementing new technology in a timely manner, providing funding and training at all levels/locations, and supporting changes is paramount for successful coordination."

2009 Quadrennial Fire Review

¹ http://www.nifc.gov/about_nifc/mission_history.htm

² Quadrennial Fire Review 2009, Executive Summary

Background

The Boise Interagency Fire Center was created in 1965 because the US Forest Service, BLM, and National Weather Service saw the need to work together in order to reduce duplication of services, cut costs, and coordinate National fire planning and operations. NPS and BIA joined the Boise Interagency Fire Center in the mid 1970s. FWS later joined in 1979. The center's name was changed in 1993 to the National Interagency Fire Center (NIFC) to more accurately reflect its National mission.³

 $^{^3\} http://www.nife.gov/about_nife/mission_history.htm$

Evaluation Results

Our evaluation determined that information technology (IT) was a critical component of firefighting operations and management. The serious deficiencies documented in this report should be addressed promptly. Future improvements in communications and technology will enhance firefighter and public safety and reduce property loss. The recommendations help mitigate current risks and prepare NIFC for the future.

The Network

The IT network at NIFC is complex and hard to manage. This makes tasks difficult to perform, indirectly encourages shortcuts that increase security risks, raises maintenance and support costs, and lowers user satisfaction. Figures 1 and 2 summarize the NIFC network as it currently exists and displays how changes to network architecture could reduce unnecessary complexity, which would reduce costs, increase efficiency, and raise user satisfaction.

High priority traffic does not have priority over routine administrative or personal network traffic because it cannot be identified and isolated. The National Interagency Coordination Center (NICC) is the focal point for coordinating the mobilization of resources for wildland fire and other incidents throughout the United States. Located on the NIFC campus, the NICC also provides intelligence and predictive services for use by the internal wildland fire community for wildland fire and incident management decision-making. With the current network design, high priority traffic related to NICC cannot be distinguished from routine network traffic supporting training, personnel management, and limited authorized personal use. Critical NICC network communications should take precedence over noncritical network traffic during high congestion.

Routine administrative and personal traffic is directed onto USDA and DOI wide area networks (WAN), potentially inducing greater network congestion and raising costs due to higher bandwidth demand. Networking resources within the NIFC campus, including cabling, are common to both the USDA and DOI. These common physical resources, however, are logically divided to maintain a technology barrier between personnel from different organizations. For example, a person from USDA physically sitting next to a person from DOI would have email routed across commercial networks supporting both the USDA and DOI, perhaps passing over the Internet, in order to transmit a single email. These barriers make it impractical to share information using typical file sharing strategies and encourage NIFC personnel to use much riskier portable hard drives (i.e. "thumb drives") to move data between organizations.

As a result, individual personnel require multiple computers connected to different networks in order to perform their job. IT support personnel estimated that 100-125 users required a computer interconnected with DOI's network and a computer interconnected with USDA's network. Acquiring and maintaining extra computer equipment raises costs and increases risk of equipment failure or security incidents. In contrast, NIFC personnel built a wireless network that is shared by all personnel at NIFC, regardless of organizational affiliation. Segmentation of network traffic is not accomplished until traffic reaches the WAN. This allows all NIFC personnel to use the same wireless access points in a common configuration and exist on the same network without local barriers.

4

⁴ http://www.nifc.gov/nicc/

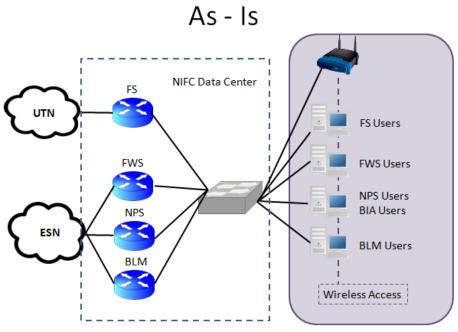


Figure 1. NIFC Network "As-Is"

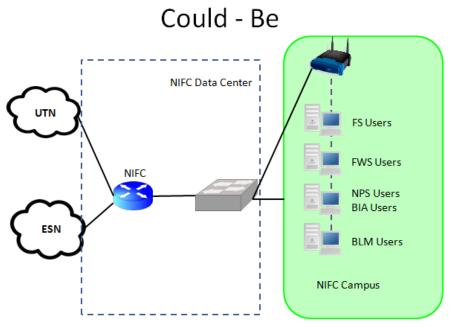


Figure 2. NIFC Network as "Could-Be"

Data Center

NIFC has a data center located on its campus. The data center has dedicated air conditioning, emergency power supply, automatic fire suppression, video surveillance, raised flooring, and other features consistent with best practices that led us to conclude it was a well-equipped facility designed for its purpose. The data center has many unused equipment racks and appears substantially underused.

Information Systems

(b) (7)(E)

is an information system that supports the NIFC mission by providing a network that hosts applications used for firefighting and fire management. The (b) (7)(E)

system is hosted on the (b) (7)(E) network and provides, among other functionality, weather information that influences decision making related to firefighting operations. The conduct of firefighting management operations relies on (b) (7)(E), yet it is not protected by the advanced technical security features provided by the Department's Enterprise Services Network.

The (b) (7)(E) application is currently categorized as a minor application with a moderate-impact rating.

(b) (7)(E) however, was formerly categorized as a major application with a high-impact rating. ⁶ A category change from high to moderate, allows for substantially less information security controls based on mandatory Federal standards. Less strict information security controls raises the risk of a security incident that could make (b) (7)(E) unavailable when needed.

We found that some bureaus did not use to report fire incidents. FWS used a minor application on the (b) (7)(E) to report fire incidents. Using disparate systems makes reporting more difficult and more costly to maintain.

Wireless Networking

The NIFC campus network uses wireless technology. The wireless network infrastructure was common to all organizations represented at NIFC. Once a wireless connection had been established between a client machine and the wireless access point, remote access protocols and equipment routed network traffic to the appropriate organizational network. This implementation demonstrates that all organizations can successfully use a common infrastructure while still accomplishing organization-specific missions.

9

.

OIG verified the C&A package for (b) (7)(E) existed and found the accreditation memo signed on 6/14/2007

Department Enterprise Architecture Repository (DEAR), September 2005 extract.

Technical Controls

Encryption of Sensitive Data

Office of Management and Budget (OMB) Directive M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006, recommends that all Departments and Agencies "encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing."

Not all DOI computers are in compliance with OMB M-06-16, which further states that Agencies must "ensure these safeguards have been reviewed and are in place within the next 45 days."

We found that both BLM and NPS implemented encryption solutions where personnel held sensitive information on laptops but determined that neither of them implemented encryption on BlackBerry devices. FWS encrypted all laptops and implemented encryption on BlackBerry devices. We did not find encryption on any BIA workstations. Moreover, BIA's BlackBerry devices did not have a password enabled or encryption installed. BIA implemented a password and encryption on their BlackBerry devices on the same day that we identified these deficiencies.

The standard workstation configuration used at NIFC applied strong policies. Weak hardware configurations, however, coupled with local administrative rights and the lack of encryption thwarted efforts to secure the workstations. We tested and confirmed that BLM and FWS workstations (b) (7)(E)

8 which could allow anyone with physical access to (b) (7)(E)

Account Management

(b) (7)(E)

We reviewed account management practices for BLM-NIFC. BLM did not fully employ existing technology to secure all user accounts. We identified user accounts created for training purposes that were

During our walk-through of one facility, we observed a username and password written on a piece of paper lying in plain view on the top of a desk (Figure 4), and we used the information to access BLM's network. While signed on to this user account, we found the previous BLM Director's email file stored on a network file share and downloaded and opened the file (Figure 5). We found that the file was not encrypted and did not require a password to access. Any user on BLM's network, including contractors, could have accessed this file.

⁷ "Booting" is the initial initialization process a computer goes through to start-up.

⁸ Computers normally "boot" from the internal hard drive. We used a CD instead so that we could issue our own instructions.



Figure 3. Username and Password

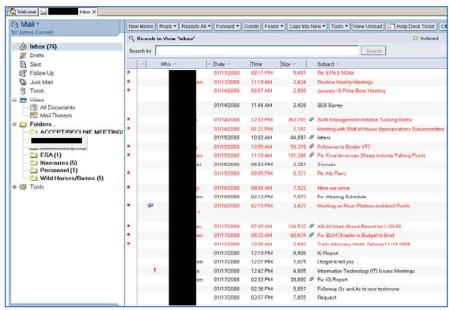
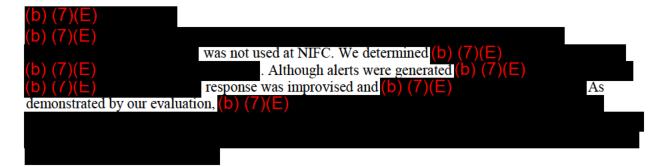


Figure 4. Previous BLM Director's Email



We conducted technical scans of computer resources from various locations around the NIFC campus and found that our activities went undetected. Unauthorized scanning activity could lead to vulnerabilities as

well as allow for identification of sensitive information; it should be considered malicious and investigated promptly when detected.

Vulnerability Scanning

We conducted technical vulnerability scanning at NIFC to detect and assess security vulnerabilities in computer resources. Our results indicate that BLM, BIA, FWS, and NPS do not patch applications and software on a regular basis. Unpatched client software is one of the most serious cyber security risks for businesses as it leaves computers open to exploitation. For example, our vulnerability scanning identified 714 vulnerabilities for one application installed throughout NIFC.

Disclosure of the technical details of vulnerabilities could place organizations at higher risk. As such, details are omitted from this report but were provided to each NIFC bureau for verification and mitigation.

Configuration Management

The Federal Information Security Management Act (FISMA) requires Agencies to comply with standards to secure information and information systems. In March 2007, OMB directed Agencies to comply with security configuration standards developed by the National Institute of Standards and Technology (NIST), the Department of Defense, and the Department of Homeland Security (DHS). These standards became the Federal Desktop Core Configuration (FDCC). In its March 20, 2007 memorandum, OMB directed Agencies to comply with FDCC standards by February 1, 2008. In March 2008, the DOI's Office of Chief Information Officer issued policy requiring all offices to be in full compliance with the FDCC standards by September 30, 2008. OMB's August 2008 memorandum, M-08-22, *Guidance on the Federal Desktop Core Configuration*, directed Agencies to meet or exceed FDCC standards regardless of the function of their workstations.

Figure 6 presents a summary of each tested FDCC benchmarks showing compliance against 100 percent of the controls to be implemented per M-08-22. We determined NIFC is merely 59 percent compliant overall with mandatory FDCC settings. We sampled a total of 18 workstations from BLM, FWS, NPS, and BIA. NPS and BIA were managed by the same policies and were on the same network, which allows BIA to utilize their network and resources.

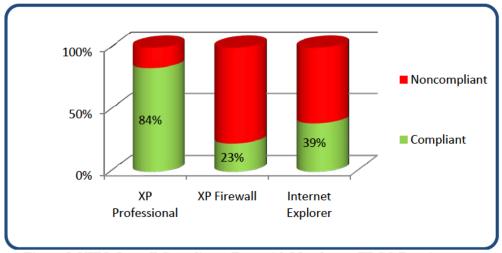


Figure 5. NIFC Overall Compliance Rate with Mandatory FDCC Requirements

We tested three benchmarks (Microsoft Windows XP Pro, XP Firewall, and Internet Explorer) and found that each bureau had an overall compliance rate of:

• BLM: 84 percent compliant;

• FWS: 67 percent compliant; and

• NPS and BIA: 28 percent compliant.

We found other applications for Web browsing, such as Mozilla Firefox, installed on workstations, allowing users to bypass mandatory security settings enabled on Internet Explorer. Utilizing a web browser which has no security settings in place increases the opportunities for hackers to access and exploit DOI workstations. Additionally, nonstandard applications, if unpatched, can lead to unrecognized vulnerabilities that can be exploited by unauthorized persons, viruses, or malicious software. In fact, unpatched client software is one of the most serious cyber security risks for businesses according to the SANS (SysAdmin, Audit, Network, Security) institute⁹.

Mandatory FDCC settings prohibit assigning escalated privileges to end-users. We found a majority of workstations at NPS and BIA gave end-users escalated privileges. Allowing end-users to have escalated privileges increases the likelihood the base image can be altered or mandatory security settings could be modified.

Firewalls provide an additional layer of security to workstations by disallowing network communications for unauthorized protocols and services. We found NPS, BIA, and FWS had the built-in Windows XP firewall on their workstations disabled. Disabling built-in security features is an example of not using available technology to its fullest potential. We found no evidence a supplemental firewall was installed at NPS, BIA, and FWS, even though FDCC requires the use of a firewall regardless of vendor. BLM had the built-in Windows XP firewall enabled on their workstations.

http://www.networkworld.com/news/2009/091609-unpatched-applications-are-top-cyber.html

Incident Detection and Response

FISMA section 3544(a)(7) requires that Agencies establish incident response capabilities and have formal procedures to detect, report, and respond to security incidents. Agencies are also required to notify and coordinate their incident response activities with the DHS's United States Computer Emergency Readiness Team (US-CERT) and notify and consult with law enforcement agencies, including their respective OIG when necessary based on the guidance. In addition, OMB July 12, 2006 memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, requires Agencies to report all incidents involving PII to US-CERT within one hour of discovering the incident.

NIST SP 800-61 Revision 1, *Computer Security Incident Handling Guide*, provides guidance for handling IT security incidents. DOI also has the *Interior Computer Security Incident Response Handbook* from June 2003.

Incidents involving the loss of sensitive information (PII) require special response procedures. All PII incidents must be reported to US-CERT within one hour of discovery. Our evaluation revealed that NIFC-BLM had established procedures for reporting and responding to IT incidents.

Multiple systems are used to report and record details of security incidents. We requested that BLM provide details of incidents that occurred at NIFC within the last 12 months from their internal repository, as well as NIFC incidents that occurred within the last 12 months recorded in the Department's incident repository. BLM was unable to provide the information at the conclusion of our evaluation. We noted that one incident potentially involving the loss of PII was not reported for nearly 3 hours after initial discovery, which violated OMB policy and Departmental policies. Multiple systems cause unnecessary latency in reporting, increase support and maintenance costs, and impede Departmental oversight.

Noncompliance with Guidance

FISMA section 3544(a) requires the Secretary of the Interior to delegate to the Department CIO "the authority to ensure compliance with the requirements imposed on the [A]gency under this subchapter." Instead, we found that guidance issued by the Department of the Interior CIO was not fully implemented.

- In May 2005, the Department CIO directed all network management transition to the Department by December 31, 2005. Furthermore, in November 2006, the Department CIO directed that the Department would procure all network services and equipment. We found BLM's(b) (7)(E) network had not yet transitioned behind the Enterprise Services Network (ESN) or turned over management of all network appliances to ESN. We were advised by NIFC personnel they were "in discussions" to transition behind ESN but no formal plan or timeline had been established.

 (b) (7)(E) hosts several important applications used to support firefighting management and operations. These applications cannot take advantage of costly and sophisticated information security technologies and are at higher risk of security incidents if they are not behind ESN.
- In August 2006, the Department CIO directed all bureaus and offices to transition to the
 Department's remote access system by January 31, 2007. We found a Cisco firewall at NIFC was
 still configured to accept remote access connections. Unauthorized remote access capabilities can
 circumvent security controls and create unmonitored connections throughout the network.

Department of the Interior Secretarial Order 3244, Standardization of Information Technology Functions and Establishment of Funding Authorities, requires that IT management be under the purview of bureau and office CIOs. We found, however, that the NIFC IT environment for BLM was under the purview of the Deputy Assistant Director for Fire and Aviation.

Our office issued a report in January 2007, ¹⁰ recommending that funding and management of radio equipment and infrastructure be consolidated under the Department CIO. Our evaluation found that the radios used in support of firefighting operations and at the NIFC campus were managed by the Assistant Director for Fire and Aviation. Management outside the purview of the Department CIO has led to use of the Department's radio systems without certification and accreditation as required by FISMA, OMB policy, and NIST standards.

.

¹⁰ C-IN-MOA-0007-2005, U.S. Department of the Interior Radio Communications Program.

Radio System

In our overview of the IT environment at NIFC, we discovered that BLM had did not have any radios with a certification or accreditation to operate. NIFC uses Land Mobile Radios (LMR) for firefighting operations as well as for routine operations including security and law enforcement. An LMR system is comprised of equipment such as handheld radios, vehicle-mounted radios, dispatch consoles, and radio repeaters. Radio traffic can be encrypted to protect communications from unauthorized eavesdropping or interference from unauthorized sources. Computer systems store encryption keys and configure the radios at NIFC for use.

Office of Management and Budget Circular Number A-130, Transmittal Memorandum 4, November 28, 2000, Appendix III, Security of Federal Automated Information Resources, Paragraph 2(c), defines a tactical radio network as a general support system and states, "Plan for adequate security of each general support system as part of the organization's information resources management planning process. The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology (NIST)."

OMB Circular Number A-130, Transmittal Memorandum 4, November 28, 2000, established the requirement to certify and accredit radio systems. More than 9 years later, radios used for firefighting and law enforcement operations were still not certified or accredited to operate.

Federal Information Processing Standards Publication

(FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, approved by the Secretary of Commerce in February 2004, is the first of two mandatory security standards required by the Federal Information Security Management Act. ¹¹ FIPS 199 states that a system is high impact if "the loss of confidentiality, integrity, or availability could be expected to have a **severe** or catastrophic adverse effect on organizational operations, organizational assets, or individuals."

FIPS 199 describes a severe or catastrophic adverse impact as "the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries." The radio system supporting firefighting, law enforcement, and security meets the high-impact criteria.

_

¹¹ FIPS 200, Paragraph 1, Purpose

Recommendations

To address deficiencies identified in this report, we recommend that:

- 1. The Department of the Interior and the U.S. Department of Agriculture should partner for coordination and consolidation of information technology resources onto a single, cohesive network.
- 2. The Department configure the NIFC network to identify and prefer high priority network traffic over routine administrative and personal network traffic.
- 3. BLM transition (b) (7)(E) behind the ESN security architecture and reevaluate the security categorization of the (b) (7)(E) system as an application with a high-impact rating.
- 4. The Department use a single system for fire reporting, as well as a single system for information security incident reporting, in order to eliminate duplication and enhance reporting.
- 5. The Department CIO assume full responsibility over the radio communications program, including management and funding of all radio equipment and related infrastructure.
- The Department certify and accredit its radio systems as high-impact systems as required by FISMA and NIST standards as well as OMB circular A-130, Appendix III, Security of Federal Automated Information Resources.
- BLM, FWS, NPS, and BIA fully implement the required FDCC settings on all computers. All NIFC bureaus should use existing technology to secure and monitor user accounts and verify and mitigate technical vulnerabilities identified by our technical security scanning.
- 8. All bureaus assign the least privilege user requirements to end users and remove administrative privileges.
- 9. All bureaus should remove unapproved software applications and standardize applications and software when possible.
- 10. BLM, FWS, NPS, and BIA should review and mitigate vulnerabilities identified from the technical scanning results provided after the evaluation.

Appendix 1: Objective, Scope, Methodology, and Related Coverage

The first objective of our evaluation was to assess the information security controls at NIFC in Boise, ID, to determine if they were implemented effectively and achieved the desired result. The second objective was to determine if information security controls were implemented in accordance with legislation, policy, and standards.

This evaluation extended to all DOI bureaus represented at NIFC, as well as their supporting information systems, including radio networks. BIA's TrustNet was not evaluated nor was the contents of any C&A packages

Other OIG audits and evaluations related to the work performed during this evaluation include:

- <u>U.S. Department of the Interior Radio Communications Program</u>, Report N. C-IN-MOA-0007-2005, January 2007. We found the Department's radio infrastructure was unsafe.
- <u>Computer Configuration Evaluation</u>, Report No. ISD-EV-MOA-0003-2009, August 2009. We found widespread noncompliance with mandatory FDCC standards and noncompliance with directives issued by the Department's CIO.
- <u>Verification of FY 2007 IT Security Recommendations</u>, Report No. ISD-EV-MOA-0002-2009, September 2009. We found management oversight of resolving the OIG information security recommendations absent and failure to fully implement a recent investment ("Cyber Security Assessment Management application") to improve information security.
- Evaluation of DOI Accountability of Desktop and Laptop Computers and their Sensitive Data,
 Report No. WR-EV-MOI-0006-2008, April 2009. We found the Department as a whole could not
 account for the computers purchased since there is no uniform policy for the tracking and chain of
 custody of portable computer equipment.
- <u>FY 2009 Federal Information Security Management Act (Revised)</u>, November 16, 2009. We found widespread noncompliance with legislation and policy.

We conducted our evaluation in accordance with the *Quality Standards for Inspections* as put forth by the Council of the Inspectors General on Integrity and Efficiency. We included tests of records and other procedures that we considered necessary under the circumstances. To accomplish our objective, we conducted the following activities:

- Reviewed applicable laws, regulations, OMB guidance, NIST standards, Government Accountability Office (GAO) reports, and Department and bureau policies;
- Reviewed documentation;
- Interviewed Department and bureau IT security personnel;
- Performed on-site inspections of bureau and office locations; and
- Performed technical testing as needed.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in government concern everyone: Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to Departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW Washington, D.C. 20240

By Phone: 24-Hour Toll Free 800-424-5081 Washington Metro Area 703-487-5435

By Fax: 703-487-5402

By Internet: www.doioig.gov

U.S. Department of the Interior Office of Inspector General



Privacy Impact Assessment Evaluation

Report No. ISD-EV-MOA-0005-2010

"The loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information."

OMB M-06-15



March 2010

Table of Contents

ACRONYMS AND OTHER REFERENCE TERMS	3
RESULTS IN BRIEF	4
INTRODUCTION	6
BACKGROUND	8
PIA ASSESSMENT	9
DOI PRIVACY INCIDENTS	18
EFFORTS TO IDENTIFY AND PROTECT INFORMATION IN IDENTIFIABLE FORM	19
PIA TRAINING	20
INFORMATION MANAGEMENT DIVISION AT DOI	21
OCIO E-GOVERNMENT REQUIREMENTS	22
RELATED AREAS IDENTIFIED DURING FIELDWORK	
RECOMMENDATIONS	25
APPENDIX 1: OBJECTIVE, SCOPE, AND RELATED COVERAGE	
APPENDIX 2: PIA ASSESSMENT CRITERIA	
APPENDIX 3: DEPARTMENT PRIVACY IMPACT ASSESSMENT TEMPLATE	29
APPENDIX 4: FIELDWORK RESULTS BY BUREAU (BIA, FWS, NBC, OS)	
APPENDIX 5: PRIVACY OFFICER ROLES BY BUREAU AND OFFICE	

Acronyms and Other Reference Terms

BIA	Bureau of Indian Affairs
	Bureau of Land Management
C&A	Certification and Accreditation
	Council of the Inspectors General on Integrity and Efficiency
CIO	
CIRC	
	Cyber Security Assessment and Management
DOI CIRC	
	Freedom of Information Act
	U.S. Fish and Wildlife Service
FY	Fiscal Year
	Inspector General
IIF	Information in Identifiable Form
	Information Security Division
IT	Information Technology
NBC	
OIG	Office of Inspector General
	Office of Management and Budget
OHA	Office of Hearing and Appeals
OHTA	Office of Historical Trust Accounting
OS	Office of the Secretary
PIA	Privacy Impact Assessment
	Personally Identifiable Information
POA&M	Plan of Action and Milestones
	SysAdmin, Audit, Network, Security Institute
	System of Record Notice
	System Security Plan
	U.S. Computer Emergency Readiness Team
	• • •

Results in Brief

We found over half of Privacy Impact Assessments (PIAs) for Information Technology (IT) systems have not been completed in a manner that would fully identify privacy risks associated with sensitive information. We found inconsistencies in the processes for PIA requirements.

A PIA is used to identify and categorize risks associated with the management of privacy data. A PIA documents the status and implementation of the requirements of Office of Management and Budget, Memorandum 03-22 (M-03-22), *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated September 26, 2003. M-03-22 states that the PIA "is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form (IIF) in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." We found DOI is not in compliance with OMB M-03-22 requirements, portions of the Privacy Act, and Departmental policies.

We examined 102 PIAs which were associated with all the accredited information systems at the Bureau of Indian Affairs, U.S. Fish and Wildlife Service, National Business Center, and Office of the Secretary. We assessed the PIA documents for completion and accuracy. We also assessed the processes for completing PIAs, maintenance of the summary data, and supporting artifacts. We found widespread and significant weaknesses in 57 percent of the 102 PIAs we assessed (See Figure 1). We determined the completion and processes of 8 percent of the PIA were good and 35 percent were determined to be satisfactory.

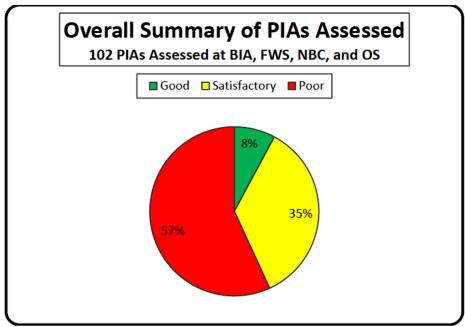


Figure 1: Summary of PIA Fieldwork

The PIAs categorized as "poor" had weaknesses in both the documents and the associated management processes. Details included in PIAs varied widely between information systems. Responses determining risk were vague, conflicting, or incomplete. When the system's approving officials use incomplete or inaccurate information, their ability to assess privacy-related risks is impaired. PIAs did not always contain approving signatures.

We found inconsistent processes for completing PIAs in various bureaus. Only some bureaus update the PIA when systems are reaccredited. We also found most general support system (GSS) PIAs did not identify all the subsystems supported by the GSS or evaluate them for privacy information. A GSS interconnects information resources that support business-related functions. Each subsystem needs to be thoroughly assessed to determine if a GSS contains IIF. The Cyber Security Assessment Management (CSAM) solution is the Department's repository for Certification and Accreditation (C&A) documentation. Data and supporting artifacts were not consistent, which hinders the bureaus' abilities to manage their IT Security Program. Inaccurate information reveals the Department's lack of oversight and hinders their ability to manage the program.

Title III of the E-Government Act, titled the Federal Information Security Management Act (FISMA), emphasizes the need for agencies to implement an organization-wide information security program. Significant overlap exists in the requirement for PIA under the Privacy Program and the IT Security Program at Interior. The programs are not organization-wide, but the Department is trying to coordinate bureau-specific programs. The sporadic implementations have resulted in inconsistent PIAs across the Department.

The Department's *Privacy Impact Assessment and Guide* was issued in 2004 and has not been updated to clarify key areas necessary to implement an effective PIA process. The outdated guidance does not clearly address a number of implementation weaknesses that we identified during this evaluation. We have included recommendations for improving guidance and the effectiveness of using the PIA as a privacy risk assessment tool.

- We found widespread and significant weaknesses in 57 percent of the 102 PIAs reviewed.
- We assessed 30 General Support System PIAs and categorized 70 percent as "poor."
- We categorized 100 percent of General Support System PIAs completed by FWS as "poor."

- The process of completing Privacy Impact Assessments is not effectively identifying privacy risk in DOI systems.
- PIAs are not completed in a timely manner or in accordance with OMB and Departmental policy.
- Departmental oversight of the Privacy Program is inadequate.

Introduction

The Department's IT Security and Information Management Programs were established to implement a number of legal requirements. Both programs consider multiple aspects of managing privacy risks associated with information systems. Privacy Impact Assessments (PIAs) are integrated with both DOI programs and used as a tool to identify and assess privacy risks.

The E-Government Act of 2002 was enacted by Congress on December 17, 2002, to improve the management and promotion of electronic Government services. It established a framework for using Internet-based information technology to improve citizen access to Government information and services. Title III of the E-Government Act, titled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide information security program that identifies, mitigates, and monitors information and information system risks.

The Privacy Act of 1974 mandates requirements and provides guidance for the collection, maintenance, use, and disposition of privacy information, also referred to in the Privacy Act as "records." The Privacy Act requires agencies to give notice to the public identifying systems which contain records. Agencies publish System of Record Notices (SORNs) in the Federal Register. The PIA is an effective tool for identifying systems containing records and identifying the Department's needs for SORNs.

Federal guidance pertaining directly and indirectly to PIAs is extensive and repeatedly emphasizes the need to protect privacy data and provide transparency. OMB Circular A-11, Section 53, *Preparation, Submission and Execution of the Budget*, is applicable to IT budget submissions. This section identifies the need to comply with OMB guidelines and the E-Government Act requirement to complete a PIA. OMB Circular A-130, Appendix 1, Section 3, *Federal Agency Responsibilities for Maintaining Records about Individuals*, details agency requirements for reviewing, reporting, and completing necessary publication as detailed in the Privacy Act.

Title II, Section 208 of the E-Government Act of 2002 requires OMB to issue guidance to agencies on implementing the privacy provisions of the E-Government Act. OMB Memorandum 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, dated September 26, 2003 (M-03-22), and effective April 17, 2003, provides guidance for implementing those privacy provisions. The guidance "directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected." M-03-22 also requires agencies to conduct PIAs for electronic information systems and collections and, in general, make them publicly available.

National Institute of Standards and Technology (NIST) published Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Revision 3, in August 2009 (SP 800-53). SP 800-53 provides recommendations and guidance for

implementing IT security controls for Federal information systems. SP 800-53's guidance further details the implementation of the IT security controls that addresses matters governed by applicable Federal laws, Executive orders, directives, policies, standards, or regulations, such as PIAs. NIST established a security control stating, "the organization conducts a privacy impact assessment on the information system in accordance with OMB policy."

The Department's IT Security Policy Handbook requires bureaus and offices to conduct PIAs in accordance with OMB policy for all information systems. Completed PIAs are required as part of the system's Certification and Accreditation (C&A) package. Additional Departmental guidance for completing a PIA is contained within the DOI Privacy Impact Assessment and Guide, issued March 1, 2004.

The DOI Privacy Impact Assessment Guide expands on the requirements of OMB-03-22 and requires a PIA for all information systems that maintain information on individuals, specifically systems containing information on employees and members of the public. DOI policy requires a PIA before an agency "develops or procures IT systems or projects that collect, maintain, or disseminate IIF from or about members of the public."

A PIA is the tool used to assess risks associated with privacy data in information systems and is used to implement the requirements of M-03-22 and the Privacy Act. It assists in ensuring that DOI is meeting its information stewardship responsibilities. M-03-22 states that the PIA "is an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining, and disseminating Information in Identifiable Form¹ (IIF) in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." IIF includes what is commonly referred to as Personally Identifiable Information (PII), but IIF has a broader definition.

DOI Departmental Manual, Part 383 includes policies and procedures for the Department's Information Management Division. The pertinent sections of the manual address Freedom of Information Act (FOIA), Privacy Act safeguards and management, and specific topics such as, the use of social security numbers. The manual identifies the bureaus' responsibilities in implementing Privacy Act requirements.

We conducted this evaluation to assess the Department's compliance with PIA requirements and guidance contained in:

- E-Government Act of 2002;
- The Privacy Act of 1974;
- NIST SP 800-53, Revision 3;
- OMB M-03-22;

¹ "Identifiable Form" - According to the OMB Memo M-03-22, this means information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

- DOI IT Security Policy Handbook [in pertinent sections]; and
- The DOI Privacy Impact Assessment and Guide.

We further assessed the implementation of the established processes and procedures for PIA requirements throughout DOI. During the evaluation, we made determinations on the quality of the assessments and completeness of requirement intents for PIAs.

Background

The Department is a cabinet-level agency of the Federal government that manages about one-fifth of the land area of the United States. DOI is the nation's principal conservation agency dedicated to protecting America's treasures for future generations by providing access to our nation's natural and cultural heritage. The Department's mission includes: conducting scientific research, providing wise stewardship of energy and mineral resources, fostering sound use of land and water resources, serving as the largest supplier and manager of water in 17 western states, conserving and protecting fish and wildlife, and offering recreation opportunities. Eight bureaus and each of DOI's Departmental offices carry out the agency's missions.

The IT system Certification and Accreditation (C&A) processes are completed at the bureau level. Privacy Impact Assessments (PIAs) are completed as part of the information systems security certification phase. NIST SP 800-37², *Guide for the Certification and Accreditation of Federal Information Systems* states, "[u]pon successful completion of this phase (certification), the authorizing official will have the information needed from the security certification to determine the risk to agency operations, agency assets, or individuals — and thus, will be able to render an appropriate security accreditation decision for the information system. "Following the security certification phase the authorizing official completes the accreditation and assumes responsibility and is accountable for the risks associated with operating an information system.

DOI included a PIA template in its March 2004 PIA Guide, which is available on the DOI OCIO Web site. We found that bureaus use variations of the DOI template to complete their PIAs. Appendix 3 contains the template used for NBC and OS systems. Its version has been modified to include the identification of subsystems. Modifying the DOI template enhances the bureau's ability to thoroughly assess privacy risks within the subsystem. The template covers multiple aspects of the IT Security Controls and Information Management processes for the system. The PIA is intended to ensure that system owners and developers have consciously incorporated privacy protections throughout the life-cycle of a system. The following information is included in the template:

- System description;
- Types of data collected;
- Records management considerations;
- Security controls protecting the data; and

² NIST SP 800-37 Revision 1 *Guide for Applying the Risk Management Framework to Federal Information Systems* was released February 2010, states "security *authorization package* documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation

³ http://csrc nist.gov/publications/nistpubs/800-37/SP800-37-final.pdf

Applicable system of record notice (SORN).

The DOI IT Security Policy Handbook states, "Bureaus and offices shall conduct Privacy Impact Assessments (PIAs) on all information systems in accordance with OMB policy." DOI expands on that policy in the DOI Privacy Impact Assessment Guide, version 03.01.04 and states "For all systems that maintain information on individuals (both employees and members of the public) the Department of the Interior requires that a PIA be completed for a DOI Information Technology (IT) Security Certification and Accreditation (C&A)."

OMB policy M-03-22 requires agencies to conduct a PIA before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form, from or about *members of the public* [emphasis added], or before initiating a new electronic collection of information in identifiable form for 10 or more persons.

PIA Assessment

We examined 102 PIAs associated with all the accredited BIA, FWS, NBC, and OS systems. See Appendix 4 for the bureau results. We assessed the PIA documents for completeness and accuracy. We also assessed the processes for completing PIAs and maintaining data and artifacts within the Cyber Security Assessment and Management (CSAM) solution. In a September 23, 2008 memorandum from the DOI CIO, bureaus were directed to use CSAM and designated it as the Department's "official repository for the development of C&A package documentation and to preserve all associated artifacts."

Appendix 2 details the PIA assessment criteria and the standards used to categorize PIAs. We categorized PIAs as "good," "satisfactory," or "poor," and found widespread and significant weaknesses in 57 percent of the PIAs reviewed. The PIAs categorized as "poor" had weaknesses in both PIA completion and in the associated management processes. Thirty-five percent of the assessed PIAs were determined to be satisfactory and 8 percent were categorized as "good." Specifically, General Support Systems (GSS) which support subsystems have not been fully assessed in the PIAs and processes have been inconsistently implemented. CSAM errors were identified and the responses to the template questions are incomplete or vague.

General Support Systems PIAs

A GSS "is an interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. 5" A GSS supports varying numbers of subsystems. A GSS accreditation boundary is dependent upon how the subsystems are grouped.

The DOI PIA guide states, "in cases where systems are networks that house information systems and do not actually collect, manipulate, or use the data in the systems they house, and

^{4 &}quot;Subsystem" is used in this context to define all components identified in the system C&A documentation as being grouped under a GSS, including: LAN, locations, sites, minor applications, and major applications. ⁵ NIST SP-800-37, Guide for the Security and Accreditation of Federal Information Systems.

where systems are evaluated and no information is maintained in identifiable form complete only Sections A and B.1 of the PIA." The completion of Section A and B.1 are also referred to as a "preliminary PIA." The guide further notes, "For the network systems above, indicate what systems are managed by this network. A separate assessment should be completed for each of those systems that interface with the network."

We assessed 30 GSS PIAs and categorized 21 as "poor" (see Figures 2 and 3). They were mostly categorized as "poor" because the subsystems "managed by this network" (GSS) had not been identified in the PIA and those subsystems had not been assessed for IIF. The typical response found in section B.1⁶ is "No, because the system only provides infrastructure for the network." Unless an individual assessment is completed and documented for each subsystem supported by the GSS, it would not be reasonable to conclude that the system has no IIF.

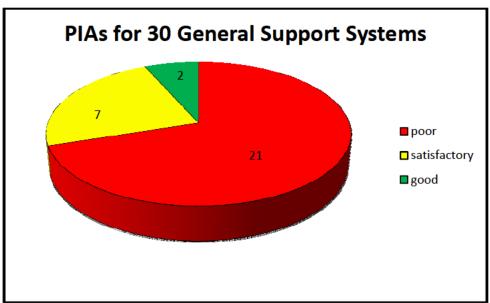


Figure 2: Categorizations of General Support System PIAs

Bureau	Number of GSSs	POOR	SATISFACTORY	GOOD
BIA	6	5	1	0
FWS	9	9	0	0
NBC	11	6	4	1
OS	4	1	2	1
Total	30	21	7	2

Figure 3: GSS PIA Completion by Bureau

GSS PIA completion was "good." The PIA identified major and minor applications supported by the GSS. The GSS further identified other PIAs that had been completed for systems on the GSS. We were able to determine from the GSS PIA if the system had been thoroughly assessed.

10

⁶ Question B.1 from the DOI PIA template: "Does this system contain any information about individuals?

In contrast, we found all nine (see Figure 3, above) of the had not assessed the minor applications for IIF. (b) (7)(E)
GSS supports its regional LANS and the (b) (7)(E)
LAN. The PIA for that system was completed December 7, 2009, and the response to question B1, "Does this system contain any information about individuals?" was, "No." The PIA fails to identify the LANs and minor applications supported by the GSS. Separate PIAs were not completed for six Regional LANs and (b) (7)(E) AN. The assessment is incomplete without a separate assessment to identify IIF within each LAN. Only (b) (7)(E) completed separate PIAs. Furthermore, human resources (HR) is decentralized, and the HR systems reside on the regional LANs, which have also not been identified and assessed for IIF. We also found the PIA artifact in CSAM for GSS was not signed, but the signature page was provided in our follow-up request.

Process Weaknesses

The system owner is responsible for preparing an accurate and complete PIA and also implementing "the legal information resources management requirements (privacy, security, FOIA, records, data administration)." System owners are not extensively trained in IT security or privacy requirements and have limited training on completing a PIA. The PIAs we examined contain extensive weaknesses that reduce any potential benefits. Completing the PIA does not effectively identify privacy risks in DOI systems.

The completion processes for PIAs created significant variation due to inconsistencies between bureaus. Almost all systems had a PIA document included in the C&A documentation. We found, however, drastic inconsistencies in the completeness and accuracy of each document's information. We found many PIAs that lacked responses or had incomplete responses to assessment questions ((b) (7)(E) (7)). We also found responses to the questions that presented conflicting or erroneous information (b) (7)(E)

PIAs are not completed efficiently and in accordance with OMB and Departmental policy. The DOI IT Security Policy Handbook states PIAs should be completed on all systems in accordance with OMB policy. OMB M-03-22 states, "[the] E-Government Act requires agencies to conduct a PIA before developing or procuring IT systems or projects." PIAs are completed at DOI as part of the C&A process and not prior to development or procurement of an IT system. We found OS had not completed a PIA for the (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

We also identified PIAs that were completed after the system accreditation (b) (7)(E)

In general, we found that most documents lacked basic quality and accuracy. Some PIAs were not dated or were missing approval signatures ((b) (7)(E) Some accredited systems did not have a PIA ((b) (7)(E)).

We found the bureaus are using multiple versions of the DOI PIA template. NBC and OS have added a section to the DOI PIA template to identify subsystems and minor applications resulting in improved completion of their privacy assessments. FWS has a variation of the DOI template

11

⁷ The acronyms in the parentheses represent the bureau and the accredited IT system and are examples of the stated condition. For more information on each IT system, see Appendix 4.

which is called a "Privacy Threshold Analysis." During fieldwork at FWS, the bureau Privacy Officer was unaware of the Privacy Threshold Analysis template.

All bureau privacy officers have multiple duties or roles beyond reviewing PIAs. See Appendix 5 for detailed listings of privacy officers' assigned roles, organized by bureau. Privacy personnel are the most qualified to provide oversight and assure PIA completeness but they do not have the necessary resources to devote to such an effort. The bureaus are not consistent in how information management roles are assigned to privacy personnel.

Privacy officers do not have access to necessary information to validate PIA accuracy because they do not have access to CSAM. Access to that information would offer more insight into the system's privacy risks. No single system, document, or person has a full view of the process as it is currently structured, which presents a challenge in ensuring the quality of PIAs in the Department.

Additionally, the Department has not performed PIA oversight to ensure the data quality or that they were uploaded into CSAM. Appendix 4 reveals the oversight inadequacies. We completed our evaluation using the same information that is available to the Department for managing the PIA process. We found obvious discrepancies, such as: unsigned PIAs, incomplete information, conflicting information, undated documents, discrepancies in CSAM dates and artifacts, duplicate artifacts, and artifacts not posted but with data entered stating the task was completed.

PIAs with Incomplete, Vague or Conflicting Information

Our review of 102 PIAs revealed that many had responses to in complete or vague answers to questions on the PIA template. We identified inconsistencies in PIAs within the same bureau as well as between bureaus.

BIA and FWS PIAs in CSAM generally had missing or conflicting information, such as dates, approving signatures, and data. We determined NBC and OS systems had accurate data and approving signatures, however, some PIAs contained vague and incomplete responses to the assessment questions.

SORNs are required under the Privacy Act and are directly associated with PIAs. We identified weaknesses in each bureau's process for correlating consistent SORN information with the PIAs and CSAM. We found SORN information was complete on most OS and NBC PIAs, when applicable, however, the information was not referenced in CSAM and SORN artifacts were not

uploaded. BIA referenced SORN IDs within CSAM and then the PIA cited a different SORN ID (5) (7)(E). BIA also had systems that cited a SORN in the PIA, but in CSAM states that a SORN was "not applicable" for the system (Document Management Program). FWS also has conflicting information in CSAM, cited as "not applicable," and PIA, which cites a SORN (Service Permit Issuance and Tracking System). All bureaus had references to SORN that was impossible to relate to the system PIAs we were reviewing. The SORN system names and the PIA system names conflict too often and the PIA did not explain the difference.

Several PIAs included vague or incorrect responses to template questions, which reflects a lack of understanding by the system owner completing the PIA and an absence of adequate oversight. Below are examples of template questions and examples of inadequate responses:

Question: Under which Privacy Act systems of records notice does the system operate?

Response examples:

- Privacy Act and the Paper Reduction Act" (b) (7)(E)
 (b) (7)(E)
- "The assignment of a System of Records Notice (SORN) Number is pending."

 (b) (7)(E)
- "There is not a current SORN number and name. We are actively working with the Privacy Act Officer to obtain this" ((b) (7)(E)
- "A new Privacy Act System of Record Notice is in process." (b) (7)(E)
- "In my opinion this is not a Privacy Act system" (b) (7)(E)

Question: What are the retention periods of data in this system?

Response examples:

- "The retention period is permanent or until the data is updated" ((b) (7)(E)).
- "Data is maintained in accordance with applicable Records Schedules, NARA and Departmental guidance for this type of data." ((b) (7)(E)

Question: Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

Response examples:

- "[T]he clauses have been inserted" ((b) (7)(E)
- "Yes, contractors are involved with the design, development and maintenance of the system." ((b) (7)(E))

Numerous PIAs and supporting artifacts contained conflicting information. Below is an example of conflicting information in the PIA, SORN, and CSAM entries for FWS. (b) (7)(E) (b) (7)(E) supports approximately 200 training center workstations which maintain records on individuals who complete training. The system security plan for (b) (7)(E) states, "Due to the nature of the information processed and stored on the (b) (7)(E), security measures must be implemented to prevent potential unauthorized disclosure."

The examples below are indicative of the detachment between system owners and bureau IT Security and Privacy personnel. Portions of the process are completed by different people, which results in conflict and confusion. Such information does not provide approving officials with sufficient information to identify privacy risks associated with the system.

- According to the PIA (see Figure 4), the system does not contain information about individuals (see Figure 5) and the PIA does not identify a SORN associated with the system (see Figure 6).
- According to the CSAM dashboard (see Figure 7), the SORN is not applicable
 even though an artifact is uploaded in the SORN field. The SORN artifact clearly
 states the system contains information about individuals (employees, the public,
 and employees of other agencies) (see Figure 8).

Relevant sections of the PIA, CSAM and SORN are presented below to demonstrate our findings.

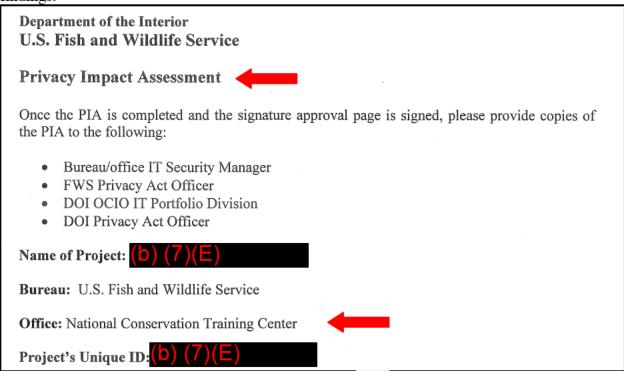
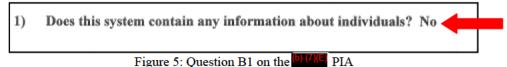


Figure 4: Identifiers on the (b) (7)(E) PIA

Question B1 on the PIA states the system does not contain information about individuals.



Question E9 on the PIA does not identify a SORN associated with the system.

9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.

Figure 6: Question E9 on the (b) (7)(E) PIA

The CSAM dashboard reflects a SORN is not applicable, yet an artifact is uploaded.

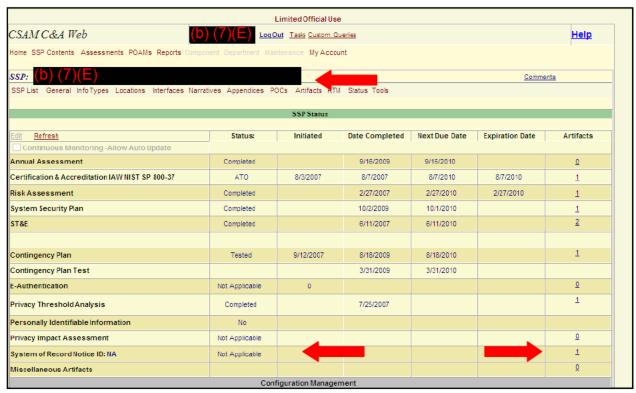


Figure 7: Screenshot of the CSAM dashboard

The relevant sections of the SORN for shown below clearly state the system has IIF for employees and the public and yet the PIA states the system does not have information about individuals.

Federal Register/Vol. 67, No. 70/Thursday, April 11, 2002/Notices DEPARTMENT OF THE INTERIOR CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM Fish and Wildlife Service Records are maintained on those individuals who participate in NCTC-Privacy Act of 1974, As Amended: sponsored training. This includes FWS Addition of a New System of Records employees as well as employees from AGENCY: Fish and Wildlife Service. other Federal agencies and non-Federal Interior. personnel from other States, private ACTION: Proposed addition of a new agencies, and universities. Training records are also kept on all FWS system of records. employees. SUMMARY: The Department of the Interior (DOI) is issuing public notice of its intent to add a new Department-wide CATEGORIES OF RECORDS IN THE SYSTEM: Privacy Act system of records to its The records contain the participant's inventory of records systems, subject to name, Social Security number. the Privacy Act of 1974. This action is organizational address, affiliation, necessary to meet the requirements of phone/fax number, email address, the Privacy Act to publish, in the lodging requirements, supervisor's name Federal Register, notice of the existence and telephone number, Federal job and character of records systems series/title/grade, billing information maintained by the agency. The new (e.g., responsible agency, tax I.D. system of records is called the "National number, agency location code (ALC) Conservation Training Center (NCTC) number, purchase order numbers, and Training Server System, FWS-34". credit card numbers), special needs, DATES: Comments on this new system of necessary course information (e.g., class) records must be received on or before titles/objectives/prerequisites, May 21, 2002. instructor(s), course leader and telephone number, start and end date/ times, minimum/maximum enrollment) class status information (e.g., class canceled/finished/scheduled, field exercise notes), and student transcripts (e.g., what course(s) each individual completed/did not complete, canceled, no-show).

Figure 8: Extracts of the Published System of Record Notice for

Another example of conflicting PIA information is BIA's (b) (7)(E)

The (b) (7)(E) security plan states the system provides electrical service utility management functions, including billing, collection, and customer account management. Multiple documents have been uploaded into CSAM, two of which appear to be duplicates, and a third document is not dated and does not have approving signatures. The information conflicts where one states the system does not have information about individuals. Another document states, "[T]he system contains information about individuals (public)."

We reviewed all BIA, FWS, NBC, and OS system Plan of Actions and Milestones (POAMs) to determine if any identified PIA weaknesses were being tracked on the system-level POAM. A system-level POAM is used to track all known IT security weaknesses. We determined that only NBC had established PIA-related POAM weaknesses for two of their systems: (b) (7)(E)

. The POAMs were created less than 30 days after we announced we would be evaluating PIAs at NBC and OS. The weakness was described as, "PIA

may incorrectly identify that no PII exists on the system. Review and update PIA as necessary to accurately reflect the state of the system as it pertains to PII."

(b) (7)(E) is an Internet accessible OS system. The public can access the Web site and search for volunteer opportunities within DOI and some non-DOI organizations. Individuals can apply online and complete a volunteer application. The application (see Figure 10) contains IIF data elements.

The system is not listed in the (b) (7)(E) the official repository for system inventory. We found the system is listed in CSAM as a major application even though it does not have a C&A package or a completed PIA (see Figure 9). Therefore, the operational system is not in compliance with OMB M-03-22 and the DOI IT Security Handbook policies which require a completed PIA during system development and is a required part of the C&A package for the system. Furthermore, potential privacy risks have not been identified and are not being managed.



Figure 9: CSAM Dashboard for (b) (7) (E)

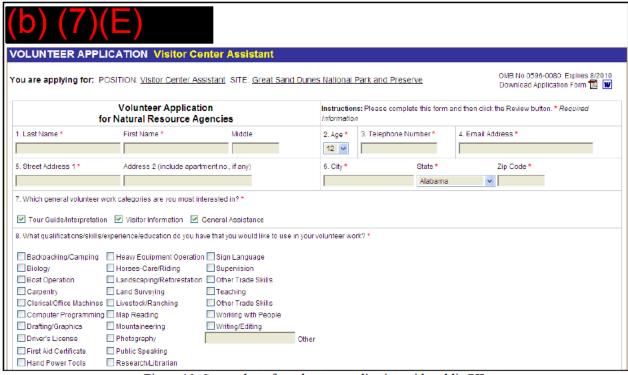


Figure 10: Screenshot of a volunteer application with public PII

DOI Privacy Incidents

In recent years, NIST, OMB, the IT Security community, and the Privacy community have all elevated the importance of managing privacy risks. OMB has issued three memoranda which emphasize agencies' responsibilities and mandate controls to mitigate potential risks. The OMB memorandums include: OMB M-07-16 (May 22, 2007, Safeguarding Against and Responding to the Breach of Personally Identifiable Information), OMB M-06-16 (June 23, 2006, Protection of Sensitive Agency Information), and OMB M-06-15 (May 22, 2006, Safeguarding Personally Identifiable Information). M-06-15 states, "the loss of personally identifiable information can result in substantial harm, embarrassment, and inconvenience to individuals and may lead to identity theft or other fraudulent use of the information. Because Federal agencies maintain significant amounts of information concerning individuals, we have a special duty to protect that information from loss and misuse."

Despite the current tools such as PIAs, DOI had IT Security events which involved Personally Identifiable Information (PII) in 2009. Thirteen DOI bureaus and offices identified and reported 568 events involving PII between January 1 and December 31, 2009. DOI's PII-related events were categorized as: lost property (PDAs, laptops, external devices, credit cards, and address listings), discovery of malicious code (e.g., Trojan horse, botnets, and adware), and user compromises. The events were reported to DOI CIRC and managed as the bureau incident-response teams deemed necessary.

OMB memorandum M-06-19, Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, was issued on July 12, 2006. M-06-19 requires agencies to report all incidents involving PII to US-CERT within 1 hour of discovering the incident. We found that 86 percent (see Figure 11) of PII events in 2009 were not reported within one hour.

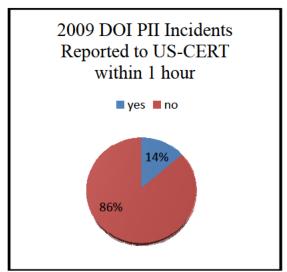


Figure 11: 2009 DOI PII Incidents Reported in Accordance with M-06-19

In our FY2009 FISMA Evaluation Report (Revised) we identified weaknesses and fragmentations in the Department's monitoring and incident response capabilities. Furthermore, we found the Department lacks adequate resources for incident response to comprehensively monitor its network for security incidents.

While detected and reported events partially reflect the magnitude of DOI security risks, undetected incidents contribute to the totality of the risk. During our Information Security Evaluation at the National Interagency Fire Center (NIFC) in December 2009, we found the former Director of Bureau of Land Management's unencrypted personal email archive file, which contained personal and sensitive information. During our walk-through at the NIFC facility in Boise, ID, we observed a training account user name and password on a piece of paper lying on top of the desk. Using that information, we accessed the BLM network, then identified and downloaded the email file. Any BLM user that authenticated to the network could have gained access to the unprotected information. This situation had not been identified prior to our NIFC evaluation and the file had been unprotected for an extended period of time. The OIG's access to the email file went completely undetected.

Efforts to Identify and Protect Information in Identifiable Form

DOI's PIAs are inadequate and have not been used to their full potential to identify systems containing IIF. However, we determined the Department, bureaus and offices do not have consistent, comprehensive, and ongoing procedures to identify and protect IIF.

The Department has partially implemented an Enterprise data loss prevention solution at three of the five main DOI Internet gateways: (b) (7)(E) The two remaining Internet gateways are implementing solutions. The current solution monitors outbound gateway traffic and includes efforts to identify PII. The solution has the capability of preventing and discovering confidential data on the network, but the necessary resources to include added functionality and management effectiveness have not been provided.

FWS uses an automated tool for bureau scanning that is capable of scanning for IIF, but they have not conducted an organization-wide scan for IIF since May 2008. NBC has a data loss prevention solution which is capable of identifying PII on workstations. However, NBC was unable to provide scan results and documentation of their mitigation efforts. They do not have a fully implemented scanning program, only a periodic implementation.

Monthly vulnerability scanning is conducted by the Department's Enterprise Services Vulnerability Management team. The objective of vulnerability scanning is to identify system vulnerabilities which could be exploited and thus the potential exists for sensitive information to be extracted. In September 2009, SANS identified Web application attacks as one of the "top cyber security risk," stating, "attacks against web applications constitute more than 60 percent of the total attack attempts observed on the Internet." Thus, Departmental scanning of Web applications impacts DOI's effectiveness in protecting IIF. The Department scans internal and external DOI IP address space and Web sites (websites.gov) which are hosted by DOI. The Department does not scan any Web sites that have dot-com domain names or other third party hosting.

One example of a dot-com application not scanned as the part of the Departmental or NBC scanning program is the (b) (7)(E) . (b) (7)(E) is hosted by (b) (7)(E) (b) (7)(E) and users access (b) (7)(E) through an Internet connection. The system is used for processing DOI equal employment opportunity (EEO) and employment discrimination complaints. The system contains sensitive information such as: settlement payments, names, titles, addresses, dates of birth, telephone numbers, disabilities, legal investigations, and social security numbers. We determined the (b) (7)(E) PIA was poorly completed and found conflicting system information when comparing the PIA to the referenced SORN.

PIA Training

The Department does not have formal training specific to PIA completion but the Departmental Privacy Office has prepared a presentation and delivered it at the OCIO-IA IT Summit in November 2009. The presentation adequately describes the PIA process and provides specific guidance for completing PIAs.

A memorandum dated April 9, 2009, titled *Release of Fiscal Year 2009 Records Management and Orientation to the Privacy Act Computer-Based Training*, was signed by the Acting Assistant Secretary for Policy, Management and Budget. The Memorandum required Record

⁸ As of March 10, 2010, the Department's data loss prevention solution is deployed at all five main DOI Internet gateways.

Management and Orientation to the Privacy Act training to be completed by all DOI employees, contractors, partners, and volunteers. In our FY2009 FISMA Evaluation Report (Revised) we reported training was completed by DOI personnel as follows: 93.7 percent completed Records Management and 81.5 percent completed Orientation to Privacy Act. Although the mandatory training pertains to PIAs, it is not designed to specifically address PIAs.

Information Management Division at DOI

The DOI Privacy Intranet Web site, available to DOI employees, is well-organized and contains comprehensive information on privacy program issues and PIAs. An abundance of information is available for information management functions, however the implementation is inconsistent and often not in compliance with policies.

The OCIO, Information Management Division (IMD) has four full-time equivalents to provide guidance and perform oversight to bureaus. The IMD division oversees Privacy, Records Management, Freedom of Information Act (FOIA) requests, Web Management / Information Collection Clearance, Section 508 (Section 508 is further described on page 25 of this report), and Information Quality. See Appendix 5 for a detailed listing of Bureau Privacy Officer's roles. There are 16 additional full-time equivalents at the bureau level who engage in many combinations of the above functions. Only BIA and BLM have dedicated Privacy Officers. Multiple roles are assigned to most bureau Privacy Officers (See Appendix 5) and the numerous demands impact the effectiveness of managing privacy related responsibilities and oversight of system PIAs.

One person is currently assigned as the OS/NBC Privacy Officer, Records Officer, FIOA Officer, and Information Collection Clearance Officer. That person also performs those duties for Departmental offices including OHA and OHTA.

During FY2009, DOI processed 5088 FOIA requests⁹. DOI makes records available to the public unless the information is protected from disclosure by one or more of the FOIA exemptions.

IMD currently has five work products underway and teams established which will specifically address some of the issues we have identified in this report. Their work products include: revising the Departmental Manual/Privacy section, revising the Privacy Loss Mitigation Strategy, revising Identify Theft Task Force and Charter, defining and reconciling systems (e-CPIC, CSAM, DEAR, C&A), and updating the Privacy Portal.

Minimum standards have not been established for DOI privacy officials. Departmental Manual Part 383, Chapter 3, details the bureaus' responsibilities to implement the requirements of the Privacy Act. The policy does not, however, establish minimum standards of competence for bureau privacy officials. Credentials are available within the field of privacy by the International Association of Privacy Professionals (IAPP). IAPP is the largest association of privacy professionals. They offer certification including Certified Information Privacy Professional/

_

⁹ FOIA, FY09 Annual report 12/16/09

Government, which is designed exclusively for employees of Federal and State government agencies.

There is not a consistent OPM series assigned to people performing privacy-related duties within DOI. The GS Series includes: GS-301- Miscellaneous Administration and Program, GS-343-Management and Program Analysis, GS-2210-Information Technology Management, Administration and Grades range from GS-12 to GS-15.

IT Security and Privacy each have roles in implementing the PIA requirements. Each of the 13 DOI bureaus has a unique organizational structure to include IT Security and Privacy personnel. BIA's Office of Information Security and Privacy is structured to allow for coordination between the Privacy, FOIA, Records Management, IT Security, and Capital Planning. During this evaluation, we found that FWS has proposed a new organizational structure which would also consolidate those types of functions under the Information Assurance Division. The DOI Privacy and IT Security Programs have not been coordinated to ensure all requirements are satisfied.

OCIO E-Government Requirements

The FY2008 OCIO E-Government Requirement document identified IT Security and Privacy as the number one priority as shown in Figure 12. Two major elements specifically relate to PIAs. The first element states, "Where appropriate, completed and approved Privacy Impact Assessments (PIAs) are in place and current for all Certified and Accredited (C&A) systems in accordance with OMB Memorandum 06-20; OMB Memorandum M-03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, dated September 26, 2003; and OMB's Proud to Be (by July 1, 2008), and the PMA scorecard." The second element to relate to PIAs states, "Systems with personally identifiable information have published Privacy Act system of records notices, in accordance with OMB Memorandum 06-20 issued July 17, 2006 Federal Information Security Management Act (FISMA) and Privacy Management; the Privacy Act; OMB's Proud to Be (by July 1, 2008) and the PMA scorecard."

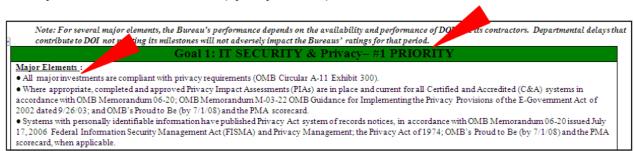


Figure 12: OCIO E-Government Requirements

E-Government — Sonny Bhagowalia Q4 2009											
Performance Indicator	BIA	BLM	BOR	FWS	MMS	NPS	OSM	USGS	OST	OHTA	NBC
IT Security and Privacy	G	G	G	G	G	G	G	G	G	G	G
Enterprise Infrastructure	Y	G	G	G	Y	G	G	G	G	G	G
Enterprise Architecture	G	G	G	G	G	G	G	G	G	G	G
IT Capital Planning & Investment	G	G	G	G	v	G	G	v	G	G	G
Control					Y			Y			
IT Workforce Management	G	G	G	G	G	G	G	G	G	G	G
Records Management	G	G	G	G	Y	G	G	G	G	G	G
Freedom of Information Act	G	G	G	G	В	G	В	G	G	G	G

Figure 13: DOI OCIO E-Government Scorecard FY2009, Quarter 4

The OCIO E-Government Scorecard for Fiscal Year 2009, Quarter 4 (see Figure 13), reflects full satisfaction of major elements on IT Security and Privacy performance indicators for all reporting bureaus. In this evaluation, we found the Department had not accomplished all PIA-related goals, yet bureaus self-reported completion.

Related Areas Identified During Fieldwork

Retired IT Systems

An accurate IT system inventory is necessary to ensure compliance with system IT Security requirements. The system inventory is foundational and impacts most aspects of the IT Security program, including the C&A package, definition of accreditation boundaries, and PIAs. The terminology used in DEAR and CSAM has not consistently been used to allow system users to clearly establish the status. We identified systems that were categorized as retired, when in reality they had been merged, transferred to new accreditation boundaries, or decommissioned. A clear distinction is important in identifying systems in each stage of its life cycle.

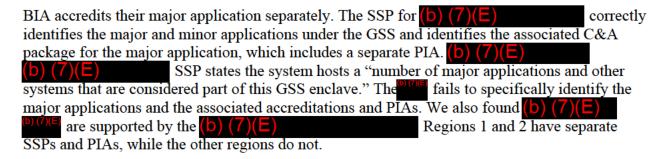
The documentation supporting system changes was not always uploaded in CSAM. Additionally, we found the memorandums submitted to the Department of the Interior Chief Information Security Officer (CISO) did not always contain adequate detail. On June 12, 2009, U.S. Geological Survey (USGS) forwarded a memorandum to the DOI CISO for the boundary decommissioning of two general support systems at the Office of Automation General and Office of Automation Specialized. The memo does not identify where the assets were transferred, the name of the new accreditation boundary, or its status.

Definition of a System

System inventory issues persist at DOI and the definitions of a "system" or "subsystem" are not used consistently. During this evaluation, we determined that "system" is used to describe accreditation boundaries, locations, sites, minor applications, GSS, major applications, SORNs, records, or LANs.

System Inventory Accreditation Boundaries

We identified inconsistencies between bureaus as to how inventory accreditation boundaries were established. FWS and NBC have major applications included in GSS accreditations while



System accreditations are required for major applications and GSSs. According to NIST 800-18¹⁰, a major application can be hosted on a general support system providing "The general support system plan should reference the major application system security plan." NIST requires all applications supported by the general support system to be identified and describe the "application's function and information processed."

Section 508 Implementation

DOI Section 508 Coordinators are responsible for organizing and supporting the Section 508 implementation for their respective bureaus. Section 508 compliance is required by the Rehabilitation Act of 1973 to ensures electronic and information technology is accessible to people with disabilities. The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology.

During the PIA evaluation, we identified the various roles assigned to personnel involved in Information Management, specifically privacy and the oversight of PIAs. During that process, we determined some Privacy Officers also assume 508 Coordinator duties. We polled all DOI bureaus to identify the bureau Section 508 Coordinators and only half the bureaus identified a person who is formally designated with that role.

OMB Budget Submissions (Exhibit 300)

OMB requires PIAs for budget submissions (Exhibit 300s) for projects maintaining information on members of the public. According to OMB M-03-22 and the DOI PIA Guide, PIAs are to be conducted during the development phase of IT systems to ensure that privacy data is identified and safeguards are considered during the design or procurement phase of the system. During this evaluation, we did not fully evaluate if adequate PIAs have been completed for all budget submissions.

The OS (b) (7)(E) major application system has been in various stages of development since 2005 and we found neither a preliminary nor a completed PIA for that system. Considering (b) (7)(E) total investment in FY06, FY07, and FY08 totaled \$26.5 million and PIAs are required at the earliest stages of development, the system should have a PIA document.

System of Record Notices: Department-wide and Government-wide Public PIAs

The E-Government Act states that each agency shall "if practicable...make the privacy impact assessment publicly available through the Web site of that agency, publication in the Federal

¹⁰ NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems.

Register, or other means." OMB reinforces this concept in M-03-22, which requires "agencies to conduct privacy impact assessments for electronic information systems and collections and in general make them publically available." Agencies may determine to not make PIA documents publically available if the publication would raise security concerns. The guidance goes on to state, "if the PIA is to be published, such information shall be protected and handled consistently with the Freedom of Information Act (FOIA)." Furthermore, "agencies may make PIA available in the Federal Register along with the Privacy Act SORNs."

DOI has a limited number of Public PIAs posted at http://www.doi.gov/ocio/privacy/ppia.html. There are approximately 180 accredited DOI systems, and 26 PIAs publicly posted. We have not conducted a full review of this difference, but there is a significant difference worth reconciling.

OS and Department-wide SORNs are posted at http://www.doi.gov/ocio/privacy/os_notices.htm. During the PIA evaluation, we were unable to establish a consistent pattern as to when Department-wide SORNs are referenced on a PIA. A number of Government-wide SORNs are posted on DOI's site at http://www.doi.gov/ocio/privacy/List_doipa_notices_9.03.htm. We also identified PIAs that cited Government-wide SORNs but again we were unable to establish a pattern as to when they were cited. We did not identify any Government-wide SORNs for any of the systems in which DOI is the managing partner for E-Government initiatives.

M-03-22 states that PIAs may be published in the Federal Register along with SORNs. We did not identify any DOI PIAs posted with the system SORNs in the Federal Register.

Recommendations

To address the deficiencies identified in this report, we recommend that DOI:

- 1. Update the DOI Privacy Impact Assessment Guide by:
 - a. Clarifying requirements for GSS and document "subsystem;"
 - b. Clarifying the use of "Privacy Threshold Assessment" or "Preliminary PIA;"
 - c. Clarifying requirements for updating PIAs;
 - d. Assuring the PIA System description correlates to the System Security Plan;
 - e. Documenting how the system was assessed for IIF:
 - f. Fully identifying specific information types and data; and
 - g. Incorporating recent OMB Privacy-related guidance (OMB-07-16, OMB-06-16, OMB-06-15).
- 2. Modify and standardize the PIA template.
- 3. Review all PIAs for accuracy, completion, and consistency.
- 4. Review PIAs, ensure valid SORNs are cited, and make certain that consistent SORN data is integrated into CSAM.
- 5. Make sure artifacts correlate with CSAM data entries.

- 6. Establish minimum standards for privacy officers including Certified Information Privacy Professional/ Government (CIPP/G) certification.
- 7. Reduce the number of roles Privacy Officers are currently fulfilling.
- 8. Improve Departmental oversight for the Privacy Program and PIA process.
- 9. Improve Departmental oversight over the CSAM application and ensure data quality.
- 10. Determine which PIAs need to be publically posted.
- 11. Ensure the E-Government scorecard is based on substantive and verified information.

Appendix 1: Objective, Scope, and Related Coverage

The objectives of this evaluation were to determine:

- If PIAs are conducted for all required information systems;
- If PIAs are complete and accurate;
- If management controls are implemented to ensure PIAs are completed consistently and promptly; and
- If privacy risks have been identified for DOI Information Systems and those risks have been identified in system PIAs.

We conducted fieldwork at the Office of the Chief Information Officer (OCIO) / Information Management and Cyber Security Divisions (CSD), National Business Center, Office of the Secretary, The U.S Fish and Wildlife Service, and Bureau of Indian Affairs. We conducted interviews with IT Security and Privacy Office personnel at the Department as well as select bureaus.

Our evaluation included an assessment of 102 PIAs for BIA, NBC, FWS, and OS accredited information systems. We obtained PIA documents for those systems and other related artifacts from Cyber Security Assessment and Management (CSAM), the Departments reporting solution and official repository for C&A packages.

Other OIG audits and evaluations related to the work performed during this evaluation include:

- <u>FY 2009 Federal Information Security Management Act (Revised)</u>, November 16, 2009. We found widespread noncompliance with legislation and policy.
- <u>Verification of FY 2007 IT Security Recommendations</u>, Report No. ISD-EV-MOA-0002-2009, September 2009. We found no management oversight of resolving OIG information security recommendations. A recent investment ("Cyber Security Assessment Management (CSAM) application") to improve information security was not fully leveraged.

We conducted our evaluation in accordance with the *Quality Standards for Inspections* as put forth by the Council of the Inspectors General on Integrity and Efficiency (CIGIE). We included tests of records and other procedures that we considered necessary under the circumstances. To accomplish our objective, we conducted the following activities:

- Reviewed applicable laws, regulations, OMB guidance, NIST standards, Government Accountability Office reports, and Department and bureau policies.
- Reviewed documentation.
- Interviewed Department and bureau IT security personnel.
- Performed on-site inspections of bureau and office locations.

Appendix 2: PIA Assessment Criteria

General Assessment Categories	Good	Satisfactory	Poor
General Support Systems (GSS)	Minor applications identified under a GSS and assessed for IIF	Minor applications are identified under GSS	GSS without identification of minor applications
System of Record Notices (SORNS) (when applicable)	SORN identified with artifact posted	SORN identified in PIA without artifact posted	SORN not identified
Timely	Timely completion and update	Timely completion	PIA not updated for more than 3 years or completed over 6 months after accreditation
Complete	PIA completed fully, good description of the data and system	PIA contains most information, all approving signatures	PIA not dated, missing information
Accuracy	CSAM data and artifacts agree	CSAM data and artifacts agree and adequate detail	Discrepancies between CSAM data and the PIA
Level of Detail	All questions on PIA addressed and data retention detailed	Most questions on PIA answered adequately	Vague responses to PIA questions

Appendix 3: Department Privacy Impact Assessment Template

Department of the Interior Privacy Impact Assessment

Month, day, YYYY(submitted to Bureau)

Name of Project:

Bureau:

Project's Unique ID (Exhibit 300):

Once the PIA is completed and the signature approval page is signed, please provide copies of the PIA to the following:

- Bureau/office IT Security Manager
- Bureau/office Privacy Act Officer
- DOI OCIO IT Portfolio Division
- DOI Privacy Act Officer

Do not email the approved PIA directly to the Office of Management and Budget email address identified on the Exhibit 300 form. One transmission will be sent by the OCIO Portfolio Management Division.

Also, refer to the signature approval page at the end of this document.

CONTACT INFORMATION:

 Who is the person complete. 	eting this document?	(Name, title,	organization.	and contact information
---	----------------------	---------------	---------------	-------------------------

- 2) Who is the system owner? (Name, title, organization, and contact information)
- 3) Who is the system manager for this system or application? (Name, organization, and contact information)
- 4) Who is the Bureau IT Security Manager (or Chief Information Security Officer) who reviewed this document? (Name, organization, and contact information)

Name

Chief, Information Security Division

Bureau

Address:

Phone:

Fax:

Email:

Who is the Bureau/Office Privacy Act Officer who reviewed this document? (Name, organization, and contact information)

Name of Bureau Privacy Officer:

Who is the Reviewing Official? (According to OMB, this is the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA)

Bureau CIO Name Bureau Chief Information Officer (CIO) Address Phone: Fax: Email:

SYSTEM APPLICATION/GENERAL INFORMATION:

- 1) Does this system contain any information about individuals {this question is applicable to the system and any minor applications covered under this system}?
 - a. Is this information identifiable to the individual¹¹{this question is applicable to the system and any minor applications covered under this system}? (If there is NO information collected, maintained, or used that is identifiable to the individual in the system, Sections C through F can be marked not applicable. If YES complete all sections for system and any applicable minor applications).
 - b. Is the information about individual members of the public {this question is applicable to the system and any minor applications covered under this system}? (If YES, a PIA must be submitted with the OMB Exhibit 300, and with the IT Security C&A documentation).
 - c. Is the information about employees {this question is applicable to the system and any minor applications covered under this system}? (If yes and there is no information about members of the public, the PIA is required for the DOI IT Security C&A process, but is not required to be submitted with the OMB Exhibit 300 documentation).
- 2) What is the purpose of the system/application?
 - 2a) List all minor applications that are hosted on this system and covered under this privacy impact assessment:

MINOR APPLICATION NAME	NIST 800-60 DATA TYPES

3) What legal authority authorizes the purchase or development of this system/application?

DATA IN THE SYSTEM:

- 1) What categories of individuals are covered in the system?
- 2) What are the sources of the information in the system?
 - a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?
 - b. What Federal agencies are providing data for use in the system?
 - c. What Tribal, State and local agencies are providing data for use in the system?
 - d. From what other third party sources will data be collected?
 - e. What information will be collected from the employee and the public?
- 3) Accuracy, Timeliness, and Reliability
 - a. How will data collected from sources other than DOI records and be verified for accuracy?
 - b. How will data be checked for completeness?

- c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).
- d. Are the data elements described in detail and documented? If yes, what is the name of the document?

ATTRIBUTES OF THE DATA:

- 1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?
- 2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?
- 3) Will the new data be placed in the individual's record?
- 4) Can the system make determinations about employees/public that would not be possible without the new data?
- 5) How will the new data be verified for relevance and accuracy?
- 6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?
- 7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.
- 8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

- 9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?
- 10) What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent?

MAINTENANCE AND ADMINISTRATIVE CONTROLS:

- 1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?
- 2) What are the retention periods of data in this system?
- 3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?
- 4) Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?
- 5) How does the use of this technology affect public/employee privacy?
- 6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.
- 7) What kinds of information are collected as a function of the monitoring of individuals?
- 8) What controls will be used to prevent unauthorized monitoring?

- 9) Under which Privacy Act systems of records notice does the system operate? Provide number and name.
- 10) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

ACCESS TO DATA:

- 1) Who will have access to the data in the system? (E.g., contractors, users, managers, system administrators, developers, tribes, other)
- 2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?
- 3) Will users have access to all data on the system or will the user's access be restricted? Explain.
- 4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials))
- 5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?
- 6) Do other systems share data or have access to the data in the system? If yes, explain.
- 7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?
- 8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other (e.g., Tribal))?

- 9) How will the data be used by the other agency?
- 10) Who is responsible for assuring proper use of the data?

See Attached Approval Page

The Following Officials Have Approved this Document

1)	System Manager		
	Name: Title:	(Signature)	(Date)
2)	Bureau Chief Information Se	curity Officer	
		(Signature)	(Date)
	Name: Title: Bureau Chief Information	on Security Officer (CISO)	
3)	Privacy Act Officer		
		(Signature)	(Date)
	Name: Title: Privacy Act Officer		
4)	Reviewing Official		
		(Signature)	(Date)
	Name: Bureau CIO Name Title: Bureau Chief Information	on Officer (CIO)	

Appendix 4: Fieldwork Results by Bureau (BIA, FWS, NBC, OS)

Bureau of Indian Affairs (BIA)

Results summary of 35 BIA System PIAs Evaluated:

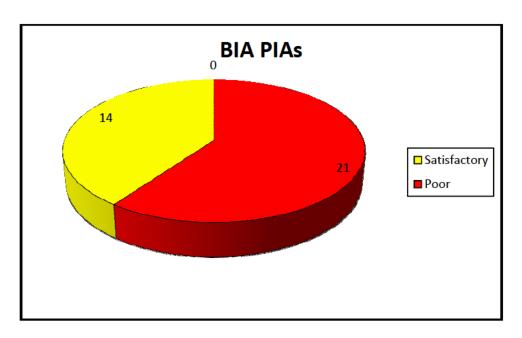


Figure 14: BIA PIA Evaluation

Detailed results of 35 BIA System PIA Evaluated:

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(b) (7)(E)	(b) $(7)(E)$			SORN error, after
(b)(/)(b)		MA	Satisfactory	accreditation
				Dated missing, conflicting
				information
		MA	Poor	
				After accreditation, vague
				responses. Example
				response: " the clauses
		MA	Poor	have been inserted"
				GSS without identification
				of minor applications, not
		GSS	Poor	updated at accreditation
				GSS without identification
		GSS	Poor	of minor applications

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(h) (7)(F)	(b) $(7)(E)$			After accreditation, CSAM
(b) $(7)(E)$				inconsistencies, same
		MA	Satisfactory	document for FMIS-EDU
				After accreditation, CSAM
		MA	Satisfactory	inconsistencies
-		IVIA	Satisfactory	CSAM discrepancies,
		MA	Poor	vague responses
		IVIA	1 001	Conflicting information,
				discrepancies, limited
		MA	Poor	detail
		1717	1 001	Not dated, no signatures
		MA	Poor	
				PIA included for (b) (7)(E),
				unable to relate to ((b)(7)(E)
				Response: Privacy Act and
				the Paper Reduction Act of
		MA	Poor	1995
				Not updated at
				accreditation, CSAM /PIA
				discrepancies, also SORN
		MA	Poor	and PIA differences
				Vague responses, system
				description, not updated at accreditation-same PIA
		540	Cathefastani	
		MA	Satisfactory	posted from(b) (7)(E)
				Vague responses- system description, not updated
				at accreditation
				at accreditation
		MA	Satisfactory	
				CSAM inconsistencies,
		MA	Poor	SORN discrepancies,
				Vague responses,
				completed after
		MA	Poor	accreditation
				(b) (7)(E) PIA uploaded as
				artifact unable to make
		MA	Satisfactory	connection to system
				Unable to make (b) (7)(E)
			-	connection to system,
		MA	Poor	lacking detail
				Lacking detail, completed
		MA	Poor	after accreditation

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(b) (7)(E)				Unable to establish status, CSAM states retired, yet ATO
	(b) $(7)(E)$	Min	Satisfactory	
				CSAM and PIA discrepancies, vague responses-system
		MA	Satisfactory	description
		MA	Poor	not updated for new accreditation, unable to determine final PIA, two artifacts posted
		GSS	Poor	GSS without identification of minor applications, CSAM and PIA discrepancies
		MA	Poor	States completed yet no artifacts. Vague response example: "in my opinion this is not a PA system."
		MA	Satisfactory	Document not dated, signatures indicate 7/28, (b) (7)(E) SORN cited-connection to (b) (7)(E)?
Pending BIA Systems			,	
				Lacking detail, CSAM and PIA discrepancies for SORN
(b) $(7)(E)$	(b) (7)(E)	MA	Satisfactory	
				Multiple documents creates confusion, data not described adequate
		MA	Poor	(b) (f)(E) PIA uploaded for
				unable to make a
				connection between the two major application
		MA	Poor	systems,

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(b) (7)(E)	(b) (7)(E)			Timely completion, PIA contains most information, all approving signatures
		MA	Satisfactory	Data in CSAM unclear based on artifacts, timely completion
		MA	Satisfactory	
				Adequate after CSAM cleanup
		MA	Satisfactory	
				GSS without identification of minor applications, not reassessed at
-		GSS	Poor	accreditation
				CSAM errors, GSS without identification of minor applications
		GSS	Satisfactory	
				Lacking detail to identify related system, many reference (b) (7)(E) SORN, document not dated unable to determine if assessed during
		MA	Poor	accreditation
Unmatched BIA Systems				
(h) (7)(F)				GSS without identification of minor applications, CSAM discrepancies
	(b) (7)(E)	GSS	Poor	

U.S. Fish and Wildlife Service (FWS)

Results Summary of 26 FWS System PIAs Evaluated

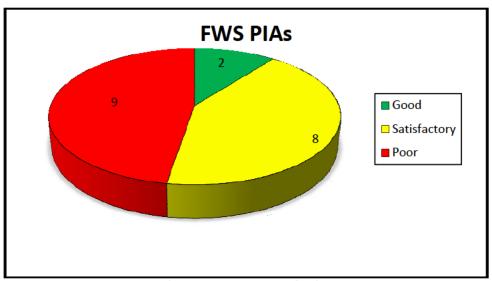


Figure 15: FWS PIA Evaluation

<u>Detailed Results of 26 FWS System PIA Evaluated:</u>

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(b) (7)(E)	(b) (7)(E)	GSS	Poor	No artifacts available- retired version, GSS without identification of minor applications
		MA	Satisfactory	Lack of detail
		MA	Satisfactory	Not updated at reaccreditation
		MA	Poor	Errors in CSAM
		Min	Poor	Errors in CSAM
		GSS	Poor	No date posted for the PIA, GSS without identification of minor applications, vague responses, Volunteer.gov the connection should be made
		МА	Poor	Errors in CSAM unable to determine actual status, after accreditation

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(b) $(7)(E)$	(b) (7)(E)	MA	Poor	Not signed, unable to determine date
		Min	Poor	Errors in CSAM unable to determine actual status- minor application or operational
		MA	Poor	Error on PTA
		GSS	Poor	No PIA, no artifacts, system accredited in 7/09, GSS w/o identification of minor applications
		GSS	Poor	No evidence the application supported by the GSS
		GSS	Poor	Unable to make a connection between public SORN and the IRN accredited system, GSS without identification of minor applications
		Min	Poor	Unable to determine from (b) (7)(E) CSAM what accreditation boundary the minor application is associated with
		MA	Poor	Errors in CSAM, unable to fully determine status listed as minor and major application
		Min	Poor	Errors in CSAM, unable to fully determine status listed as minor and major application
		MA	Good	SORN identified with artifact posted, PIA completed fully, good description of
		GSS	Poor	GSS without identification of minor applications

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(b) (7)(E)	(6) (7)(E)	GSS	Poor	PIA and SORN present conflicting information, GSS without identification of minor applications
Pending FWS Systems (systems associated with pending)				
(b) (7)(E)	(b) (7)(E)	MA	Poor	Approving signatures unsigned, missing information-use TBD on the PIA
		MA	Satisfactory	Errors in CSAM, most information included on PIA
		MA	Satisfactory	Most questions on PIA answered adequately
		MA	Poor	No artifacts in CSAM
		MA	Satisfactory	SORN artifact missing in CSAM
		GSS	Poor	GSS without identification of minor applications, inconsistencies in Regional LAN, no signatures until requested
Unmatched FWS Systems				
(b) (7)(E)	(b) (7)(E)	GSS	Poor	GSS without identification of minor applications, no artifacts in CSAM

National Business Center (NBC)

Results Summary of 19 NBC System PIAs Evaluated

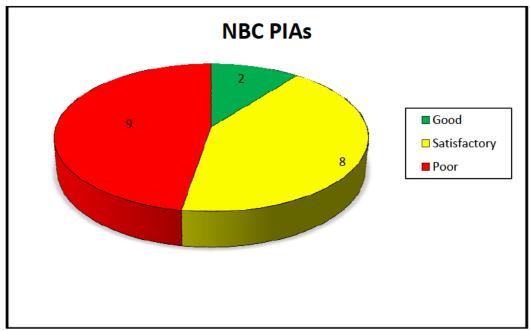


Figure 16: NBC PIA Evaluation

Detailed Results of 19 NBC System PIA Evaluated:

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(b) (7)(E)	(b) (7)(E)	GSS	Poor	No artifacts available- retired version
(b) (/)(E)		GSS	Good	Incomplete-lack of detail
		MA	Good	Not updated at reaccreditation
				Minor application-unable to determine what accreditation boundary
		GSS	Poor	the system is associated with
		GSS	Satisfactory	Minor application identified however does not state if PII is present
		MA	Satisfactory	No artifacts available that link to the cited SORN

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application	Adequacy of PIA or PTA	Comments
,		Туре	completion	
				Lacks clarity-reference to
				major applications
(h) (7) (E)				hosted and reference to
(b) $(7)(E)$	(b) (7)(E)			OPM without adequate
() () ()	(b) (1)(E)	GSS	Poor	detail
				SORN not identified and
		MA	Poor	not artifacts
		ccc	,	Added to CSAM
		GSS	n/a	prematurely
				Inadequate detail- minor
				application and
				assessment not
		CCC	Poor	completed (note POAM established)
	_	GSS	Poor	SORN identified - No
		GSS	Catisfactory	SORN artifacts
	-	033	Satisfactory	
				Minor application identified-lacks adequate
				detail, references
		МА	Satisfactory	SORNS-yet no artifacts
		IVIA	Satisfactory	SORN not completed
				timely- states in
				progress, yet accredited
		MA	Poor	over 18 months ago
			. 55.	Vague response-data
		MA	Satisfactory	retention
				Timeliness issues-states
				old version, minor
		GSS	Poor	application not identified
				We were unable to
				determine from (b) (7)(E)
				CSAM what accreditation
				boundary the minor
				application is associated
(b) (7)(E)	(b) (7)(E)	MA	Poor	with
	Unable to			
	identify			
	what this			
D. II. NDCC	system	ccc		
Pending NBC Systems	included	GSS	Undeterminable	

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(b) (7)(E)	(b) (7)(E)			Incomplete information- states SORN needs to be developed cannot
(3) (3)(-)		GSS	Satisfactory	determine status
		GSS	Satisfactory	Vague response-data retention
				SORN identified - No
		MA	Satisfactory	SORN artifacts
	Unable to identify what these system			
Unmatched NBC Systems	include	GSS	Undeterminable	
(b) (7)(E)	(b) (7)(E)	CSS	D	Minor application and assessment not
(D)(I)(E)	(b) (7)(E)	GSS	Poor	complete

Office of the Secretary (OS)

Results Summary of 22 OS System PIAs Evaluated:

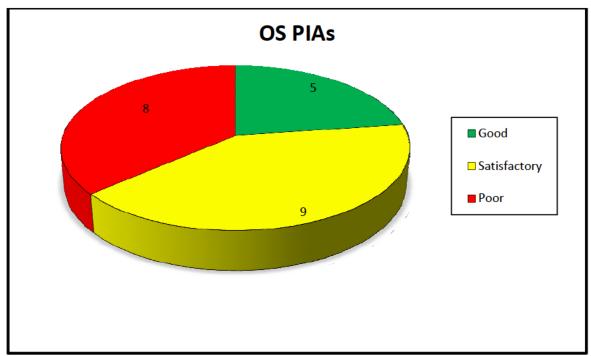


Figure 17: OS PIA Evaluation

Detailed Results of 22 OS System PIA Evaluated:

C&A Boundary Name (obtained from DEAR)	Acronym	Security Application Type	Adequacy of PIA or PTA completion	Comments
(b) $(7)(E)$	(b) (7)(E)	MA	Satisfactory	Incomplete – system description
()()		MA	Good	Timely, complete, approving signatures
				Timely, complete, approving signatures, record retention
		MA	Good	detailed
		GSS	Good	Completeness- includes PIA for (b) (7)(E) and describes the separate GSS and MA and the associated PIAs for those systems
				Timely, complete, approving signatures,
		MA	Good	adequate detail

				SORN identified - No
(b) (7)(E)	(b) $(7)(E)$	240	Catiofastana	SORN artifacts
	(~) (.)(—)	MA	Satisfactory	SORN identified - No
	-	MA	Satisfactory	SORN artifacts
				SORN identified - No
				SORN artifacts-
				signature missing on
				the March 2007
				version, provided
				Nov 2009 with
		GSS	Satisfactory	signatures
				CSAM updates
				needed for name
				change, updated
				PIA is posted under
		GSS	Satisfactory	(b) (7)(E)
				SORN identified - No
		MA	Satisfactory	SORN artifacts
				SORN not cited in
				CSAM, no SORN
		MA	Satisfactory	artifacts
T T			•	SORN identified with
				links in the PIA
				document-links
		MA	Satisfactory	broken
†			,	Name change not
				documented
				adequately, SORN
				identified - No SORN
				artifacts
				(Government-wide
		MA	Poor	SORNs cited)
+		1407	1 001	Inconsistencies in PIA
				and SORN-different
				summaries of data in
				the system, system
				name changes not
		MA	Poor	clear
+		IVIA	1 001	PIA not completed,
		0.40	D	development system
		MA	Poor	
				PIA states SORN in
				process, posted in
		0.40	D.	CSAM almost 3 years
		MA	Poor	after PIA completion
				Timely, complete,
				approving signatures,
		MA	Good	adequate detail
Pending OS Systems				
				PIA states SORN is
(b) $(7)(E)$				Pending, no SORN
	(b) (7)(E)	MA	Poor	artifacts or status

				update in CSAM-
				external customers
				accessing (b) (7)(E) are
				they citing a DOI
				SORN?
				SORN identified - No
				SORN artifacts in
(b) (7) (F)	(b) $(7)(E)$			CSAM, however
(b) $(7)(E)$		MA	Satisfactory	posted on DOI site
				PIA not updated
				when reaccredited,
				outdated PIA
		ccc		guidance cited in the
		GSS	Poor	PIA (2002)
Unmatched OS Systems				
				PIA not completed-
				added to CSAM,
				not included in
				(b) (7)(E) no C&A or
				PIA artifacts,
				system has been
(h) (7) (F)	?	Min	Poor	deployed
(b) $(7)(E)$				PIA not completed-
				no C&A or PIA
				artifacts, systems
	?	MA	Poor	are deployed

Appendix 5: Privacy Officer Roles by Bureau and Office

Departmental and Bureau Privacy Personnel	Number of Roles	Privacy	IT Security	Records Mgt. Officer	FOIA	Information Collection Clearance Officer	508 Coordinator	Information Quality Officer
Senior Agency Official								
for Privacy	Dedicated	X						
Departmental Privacy								
Specialist	Dedicated	Х						
Departmental Privacy								
Specialist	Dedicated	Х						
Departmental Privacy								
Specialist	Dedicated	X						
Assistant Secretary								
for Indian Affairs & Bureau of Indian								
Affairs	Dedicated	Х						
Bureau of Land	Dedicated							
Management	Dedicated	х						
Bureau of	Dedicated							
Reclamation	4	х			X		Х	X
Fish and Wildlife								
Service	3	X		X	X			
Minerals								
Management Service	2	X			X			
National Park Service	2	Х	Х					
Office of the								
Secretary/National								
Business Center	4	Х		X-acting	X-acting	Х		
Office of Surface								
Mining	3	Х		X	X			
Office of the Solicitor	3	X		X	X			
U.S. Geological								
Survey	3	X		Х	X			
Office of Hearings		v						
and Appeals	No response	Х						
Office of Historical	N4	v	v		v	v	v	v
Trust Accounting	More than 4	Х	Х		Х	Х	Х	X
Office of the Special Trustee	2	Х		х				
Trustee	Z	^		^				

Report Fraud, Waste, Abuse And Mismanagement



Fraud, waste, and abuse in government concerns everyone:
Office of Inspector General staff,
Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or Insular area programs and operations. You can report allegations to us in several ways.



By Mail: U.S. Department of the Interior

Office of Inspector General Mail Stop 4428 MIB 1849 C Street, NW Washington, D.C. 20240

By Phone: 24-Hour Toll Free 800-424-5081

Washington Metro Area 703-487-5435

By Fax: 703-487-5402

By Internet: www.doioig.gov

Revised 06/08



United States Department of the Interior

Office of Inspector General

Washington, D.C. 20240

Memorandum

To:

Sanjeev Bhagowalia

JAN 22 2010

Chief Information Officer, Department of the Interior

From:

Eddie Saffarinia

Assistant Inspector General for Information Technology

Subject:

Management Advisory - Insecure Web Site

On January 19, 2010, we found the Department's web site "www.doi.gov" was not securely configured.

Our testing revealed that the configuration of the Department's web site made it vulnerable to malicious parties. For example, with minimal effort, we determined the type and version of software running on the server hosting the Department's web site. With this information, malicious parties can direct targeted attacks specific to the platform hosting the Department's web pages or exploit newly discovered vulnerabilities before those vulnerabilities can be patched. Some vulnerabilities may go undetected and unreported for weeks and could make the Department's web site open to attack for an extended period of time.

We also accessed the administrative login pages for the content manager and web server management console. Both of these portals also identify the type and version of software being used to support and manage the Department's web site. Neither of these login pages should be accessible by the public.

In addition, we were able to view and download scripts used to support the web site. Malicious parties frequently analyze such scripts in detail to find vulnerabilities that can be further exploited. Best practice is to restrict public access to such information.

After determining that we could access areas of the web server not intended for public access, we discontinued testing to avoid disrupting the Department's operations and to permit immediate notification of these findings. We recommend the Department immediately secure its web site by conducting a thorough vulnerability scan and penetration test in order to ensure all weaknesses have been identified and mitigated.

We ask that you apprise us within 30 days of the date of this memorandum of the actions you take or plan to take in response to this Management Advisory. If you have any questions, please contact me at 703-487-5369. Staff may contact Michael Ashworth, Director of Information Security Division at 703-487-5360.

cc: Deputy Assistant Secretary, Technology, Information, and Business Services



U.S. Department of the Interior Office of Inspector General

AUDIT REPORT

MAINFRAME COMPUTER
POLICIES AND PROCEDURES,
ADMINISTRATIVE SERVICE CENTER,
BUREAU OF RECLAMATION

REPORT NO. 97-I-683 MARCH 1997



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

MAY - 5 1997

MEMORANDUM

TO:

The Secretary

FROM:

Wilma A. Lewis Inspector General

SUBJECT SUMMARY:

Final Audit Report for Your Information - "Mainframe

Computer Policies and Procedures, Administrative Service

Center, Bureau of Reclamation" (No. 97-I-683)

Attached for your information is a copy of the subject final audit report. The objective of the audit was to evaluate the adequacy of the management and internal controls of the mainframe computer system and processing environment of the Bureau of Reclamation's Administrative Service Center. Specifically, the audit focused on management and internal controls over the following areas: computer center management and operations; telecommunications and local area network security; application systems access; mainframe computer system physical and logical security; and contingency planning, backup, and disaster recovery.

We identified 15 weaknesses in the areas reviewed and made 24 recommendations for improving management and internal controls at the Service Center.

Based on the Bureau's response, we considered 13 recommendations implemented and 10 recommendations resolved but not implemented and requested the Bureau to reconsider the remaining recommendation, which related to improving internal controls over access to the mainframe computer.

If you have any questions concerning this matter, please contact me at (202) 208-5745 or Mr. Robert J. Williams, Assistant Inspector General for Audits, at (202) 208-4252.

Attachment

GLOSSARY

Asynchronous Protocol. Refers to a set of conventions used to start and stop transmissions that occur without a regular or predictable time relationship to a specific event. Synchronous protocol refers to a set of conventions used for transmissions that occur regularly or predictably with respect to a specific event.

Customer Information Control System (CICS). This is an IBM software product that serves as a teleprocessing monitor for the MVS operating system on the Service Center's mainframe computers, which enables transactions entered at remote computer terminals to be processed concurrently and is designed to control execution of application programs in an interactive on-line environment.

Data Structure. How the data are physically laid out within a computer system (for example, the fields in a record).

Ethernet. A networking scheme that allows microcomputers to be connected to a network. It physically consists of cabling, which connects all the machines on a network.

Multiple Virtual Storage/Enterprise Systems Architecture (MVS/ESA). An operating system that runs on IBM mainframe computers and increases virtual memory capability to 16 terabytes (trillion bytes),

Resource Access Control Facility (RACF). An IBM-licensed product that provides for access control by identifying and verifying users to the system, authorizing access to protected resources, logging detected unauthorized attempts to enter the system, and logging detected accesses to protected resources.

Time Sharing Option (TSO). A system software product that serves as the session manager on the mainframe computers whereby terminal users can submit jobs on-line. Time sharing allows a number of users to execute programs concurrently and to interact with the programs during execution.

Transmission Control Protocol/Internet Protocol. The system that networks use to communicate with each other by allowing traffic to be routed from one network to another. The Internet Protocol is a set of conventions used to pass packets (that is, a cluster of data) from one network to another.



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL

Washington, D.C. 20240

MAR 3 | 1997

AUDIT REPORT

Memorandum

To: Assistant Secretary for Water and Science

From: Robert J. Williams

Assistant Inspector General for Audits

Subject: Audit Report on Mainframe Computer Policies and Procedures, Administrative Service

Center, Bureau of Reclamation (No. 97-I-683)

INTRODUCTION

This report presents the results of our audit of mainframe computer policies and procedures at the Bureau of Reclamation's Administrative Service Center. The objective of the audit was to evaluate the adequacy of the management and internal controls of the Service Center's mainframe computer system and its processing environment. Specifically, the audit focused on management and internal controls over the following areas: computer center management and operations; telecommunications and local area network (LAN) security; application systems access; mainframe computer system physical and logical security; and contingency planning, backup, and disaster recovery.

BACKGROUND

The Bureau of Reclamation's Administrative Service Center in Denver, Colorado, provides: (1) consolidated payroll and personnel services for about 106,000 employees in the Department of the Interior and five other Federal agencies and (2) Government accounting, integrated budgeting, and reporting services through the Federal Financial System (FFS) to five Departmental and five other Federal agencies.

At the time of our review, payroll and personnel services were provided through the Payroll/Personnel System (PAY/PERS). However, the Service Center was developing a new personnel/payroll system, the Federal Personnel Payroll System (FPPS). The first phase of the new system, which has been implemented, is the SF-52 System (an SF-52 form is entitled "Request for Personnel Action"). The second phase, which consists of personnel actions and payroll processing, is scheduled for implementation beginning in September 1997. The Service Center was also to provide payroll and personnel services to an additional 65,000 Social Security Administration employees beginning in October 1997.

The Service Center's ADP Services Division is responsible for managing the computer center that provides the various services. To assist the Division in carrying out its functions, the Service Center has contracted Tri-Cor to provide staff to assist in operating and maintaining the computer systems software, communications, and LANs. The computer center provides data processing support for several sensitive systems, including PAY/PERS, FFS, SF-52, and FPPS. To support these systems, the computer center operates an IBM mainframe computer that runs Multiple Virtual Storage (MVS) Extended Systems Architecture operating system to manage the processing work load. The access control security software installed on the mainframe computer is the Resource Access Control Facility (RACF), which controls user access not only to the application systems, such as the Customer Information Control System applications, but also to the Time Sharing Option (TSO) facility. The FFS contains application level security that controls the action a user may invoke. Other system software, such as other data base management software, telecommunications software, and specialized vendor software products, also resides on the mainframe computers. Network and local communications support for both asynchronous and synchronous protocols are provided, as well as LAN connectivity, through Ethernet and Transmission Control Protocol/Internet Protocol. (The specific computer system software and network communications cited are detailed in the Glossary.)

SCOPE OF AUDIT

To accomplish our objective, we interviewed Service Center and Tri-Cor personnel, reviewed systems documentation, observed and became familiar with computer center operations and data structures, analyzed system security, and observed a disaster recovery test. In addition, we reviewed the software maintenance procedures. Because our review was limited to evaluating the adequacy of internal controls at the Service Center, we did not test the effectiveness of the internal controls at the various bureaus and agencies serviced by the Service Center.

Our audit, which was conducted during June through October 1996, was made in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we evaluated the Service Center's system of internal controls over its mainframe computer system that could adversely affect the data processing environment, The control weaknesses that we found are discussed in the Results of Audit section and in Appendix 1 of this report. If implemented, our recommendations should improve the management and internal controls in the areas cited.

_

¹According to the National Institute of Standards and Technology, sensitive systems are defined as "systems that contain any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

PRIOR AUDIT COVERAGE

During the past 5 years, the General Accounting Office has not issued any reports related to the scope of this audit. However, in March 1994, the Office of Inspector General issued the report "Compliance With the Computer Security Act of 1987, Denver Administrative Service Center, Bureau of Reclamation" (No. 94-I-357). The report stated that the Service Center generally complied with requirements of the Computer Security Act of 1987 but that improvements were needed in the areas of security and operations. Since the Service Center was addressing all of the deficiencies identified, no recommendations were made. However, deficiencies in performing a risk analysis of the Service Center's LANs and in the separation of duties within RACF software still existed during our review. These issues are discussed in the Results of Audit section and in Appendix 1 of this report.

RESULTS OF AUDIT

The Bureau of Reclamation's Administrative Service Center has weaknesses in management and internal controls in five major areas: (1) computer center management and operations; (2) LAN protection; (3) FFS application; (4) computer mainframe system physical and logical security; and (5) contingency planning, backup, and disaster recovery. Office of Management and Budget Circular A-130, "Management of Federal Information Systems," and the National Institute of Standards and Technology Federal Information Processing Standards Publications require Federal agencies to establish and implement computer security and management and internal controls to improve the protection of sensitive information in the computer systems of 'executive branch agencies. Additionally, the Congress enacted laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls is adequate. However, the Service Center has not complied with these criteria in that it did not document formal policies, standards, and procedures; follow proper practices and processes; segregate duties; comply with key software vendor guidelines for MVS integrity; and develop a formal, up-to-date, comprehensive data security program. These weaknesses increase the risk of unauthorized access and modifications to and disclosure of client-sensitive data supported by the Service Center's mainframe computer; theft or destruction of hardware, software, and sensitive information; and the loss of critical systems and functions in the event of a disaster.

Overall, we identified 15 weaknesses and made 24 recommendations for improving management and internal controls at the Service Center. The weaknesses within the five major areas are provided below, and specific details of the weaknesses and our respective recommendations to improve these weaknesses are in Appendix 1.

Computer Center Management and Operations

We found that contractor employees in critical positions did not have proper background clearances, Without knowledge of security-related background information on contractor personnel, the risk is increased for Service Center's sensitive systems to be compromised. We made one recommendation to address this weakness.

LAN Protection

We found that the Service Center could improve controls in administering and managing its LAN. Improved controls were needed in the areas of intruder detection lockout settings, disaster recovery, and user access. Because of the weak controls, the risk is increased for Service Center personnel to have unauthorized access to the mainframe computer and thus to sensitive payroll and accounting data. We made five recommendations to address these weaknesses.

FFS Application

We found that access controls in the FFS application software would not prevent Service Center users from generating unauthorized disbursements. Specifically, several users had access to vendor tables, which could result in the tables being changed and disbursing documents being affected. We made one recommendation to correct this weakness,

Mainframe Computer System Physical and Logical Security

We found that the Service Center did not always comply with Circular A- 130 or the Department of the Interior's "Information System Security Handbook." Also, the Service Center did not implement controls recommended in software vendor guidelines and generally accepted information system industry practices in administering and implementing operating system and access security software on its mainframe computers. These weaknesses were in the areas of physical security, password settings, System Management Facility (SMF) logs, multiple user identification (ID) codes, ADP access levels, separation of duties in the use of RACF security controls, and computer security plans. As a result, sensitive data maintained on the Service Center's computer were vulnerable to unauthorized access and change. We made 14 recommendations to address weaknesses in these areas.

Contingency Planning, Backup, and Disaster Recovery

We found weaknesses in the Service Center's contingency planning, backup, and disaster recovery for its sensitive systems and mainframe computing environment. Specifically, rather than relying on documented procedures, the Service Center relied upon individuals' knowledge. We also found that the Service Center did not have a documented comprehensive business recovery plan. As a result, in the event of a disaster, the Service Center may not be able to recover critical systems and business functions. We made three recommendations to address these weaknesses.

Bureau of Reclamation Response and Office of Inspector General Reply

In the March 24, 1997, response (Appendix 2) from the Commissioner, Bureau of Reclamation, to our draft report, the Bureau generally concurred with 23 of our 24 recommendations. Based on the response, we consider Recommendations A.1, D.1, D.2, E.1, F.1, F.2, F.3, H.1, H.2, I.2, J.2, M.1, and N.1 resolved and implemented; Recommendations B.1, C.1, D.3, G.1, G.2, I.1, J.1, K.1, N.2, and 0.1 resolved but not implemented; and Recommendation L. 1 unresolved. Accordingly, the unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation, and the Bureau is requested to reconsider the unresolved recommendation (see Appendix 3). While the Bureau's response generally concurred with the recommendations, except for Recommendation L. 1, the response did take issue with several statements regarding our recommendations, which we have addressed as follows:

- Recommendation L.1. The Bureau said that it "disagree[d]" with the recommendation and that it "question[ed] any adverse effect as well as any benefit from retroactively requiring additional documentation [to ensure that Decentralized Security Administration Facility records are updated for oral access adjustments]. While we did not question the validity of oral requests for access to the mainframe computer systems, we did recommend that these requests and approvals be documented in Facility records to allow reconciliation between access requested and access allowed to ensure that access is assigned at the appropriate level. Accordingly, the Bureau should reconsider its response to this recommendation.
- Recommendation F.1. While the Bureau said that it has complied with the recommendation, it stated that the problem was "currency of documentation" and not a problem of physical security because two levels of security control occur before personnel are allowed entry into the computer rooms. We agree that two levels of security control had to be passed through to enter the computer room. However, the Service Center had "generic" key cards that were issued to and used by vendors and building management personnel for access to the computer rooms. Thus there was little assurance that only specific people had use of the key card to gain access to the computer rooms.
- Recommendation G.2. While the Bureau said that it concurred with the intent of the recommendation, it stated in its response that the 180-day password interval for RACF security applied to only one application, the Automated SF 52 System. The Bureau stated that the "extended interval" was requested by the users and approved by the Bureau's Security Manager. It further disagreed with our assertion that "not all mainframe applications have access security." We disagree with these statements. First, the Automated SF 52 System is not the only application residing on the mainframe. The mainframe also houses the PAY/PERS and the Federal Financial System, both sensitive applications. Further, at the time the Service Center received approval for the 180-day password interval in June 1994, the PAY/PERS was not residing on the mainframe. Second, the PAY/PERS does not have adequate security within the application; thus it relies exclusively on

RACF security to control access. As such, by default, users to the mainframe applications have 180-day password settings.

- Recommendation K.1. While the Bureau concurred with the recommendation, it disagreed that the condition was caused by the limited number of staff assigned to the group for monitoring security. The Bureau stated, "This information does not represent the ASC [Administrative Service Center] position." During our review, we found that the group did not have an adequate number of staff or that the work load was distributed to ensure that the segregation of duties was adequate.
- Recommendation N.1. While the Bureau concurred with the recommendation, it stated that "this condition should have been more appropriately stated as a currency of documentation issue" because the Administrative Service Center "has addressed recovery of the Federal Financial System and telecommunications although not formally documented." We disagree. By not including the Federal Financial System and telecommunications in the Continuity of Operations Plans, there is little assurance that the Federal Financial System and telecommunications would be addressed and recovered during the testing of the plan or in the event of a disaster. Further, during our review of a disaster recovery test, the Federal Financial System was not included in any of the tests performed by the Service Center.

Additional Comments on Audit Report

In its response, the Bureau disagreed with our use of "generally accepted industry and information system standards" as acceptable criteria, stating that "a conclusive set of standards were not available and the auditors were not aware as to whether these standards had ever been issued as official Government-wide policy." The Bureau further stated that the Department's Office of Information Resources Management had likewise advised that it was unaware of these standards and of their applicability to Departmental organizations,

However, computer and information system audit guidelines that were used by the auditors in performing the audit are those that are also used by other Federal Government and private industry auditors and computer installation staff in evaluating the effectiveness of computer center management and operations, The audit guidelines refer to numerous directives, policies, and guidelines issued by the Office of Management and Budget and the National Institute of Standards and Technology and, by reference, to non-Federal standard-setting organizations such as the Information Systems Control Foundation, the Institute of Internal Auditors Research Foundation, and the American Institute of Certified Public Accountants. Further, the Office of Management and Budget and the National Institute of Standards and Technology, by reference, include and recognize not only these non-Federal standard-setting organizations but also the British Standards Institute, as well as: (1) periodicals such as the Auerbach Publishers newsletters and articles (EDP Audit and Control Newsletter), LAN Times, and Infosecurity News; (2) symposiums and conferences held by the Institute of Electrical and Electronic Engineers Computer Society, the National Computer Security, and UNIX; and (3) individuals who are considered experts in information systems such as the Inspector General for the U.S. House of Representatives. While guidelines and standards issued

by these organizations, publishers, and individuals may not have been issued as "official Governmentwide policy," they promulgate industrywide standards and are the bases for many Governmental directives, policies, and guidelines issued that are related to information systems. In addition, many of the Federal Government policies, directives, and guidelines state that the requirements therein are "minimum" requirements, which implies that additional requirements or standards such as those defined by the information systems industry can and should be used.

The Bureau also questioned certain recommendations in terms of their consistency with Office of Management and Budget policies, in particular, with policies of Circulars A-123 and A-1 30. In this regard, the Bureau said that we did not consider cost as an "important consideration" when addressing "adequate" computer security controls.

Regarding the "costs" of our recommendations, we are not responsible for performing cost-benefit analyses of the computer controls needed for the Bureau's automated information systems. Rather, the Bureau is responsible for conducting an adequate review of the risks and associated costs when it determines the controls needed in its computer systems, The auditors are responsible for determining whether the analyses were adequate for the circumstances. During our review, the Bureau could not provide us with any such analyses of cost versus risk.

While the Bureau stated that armed guard service was on-site at the Service Center 24 hours a day, we did not see a guard on-site during normal duty hours at any time during our audit. We agree that the security measures identified in the Bureau's response reduce the risk of physical damage to the Facility and thus to computers. However, our audit was not limited to reviewing only the physical access to and the security of the Facility. It also included a review of physical access to computer hardware and software. As stated in our report, physical access to the computer rooms was not controlled or limited to only those personnel who required access to perform their day-to-day duties.

As required by the Departmental Manual (360 DM 5.3), please provide us with your written comments to this report by June 3, 1997. The response should provide the information requested in Appendix 3.

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Bureau Administrative Service Center personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

COMPUTER CENTER MANAGEMENT AND OPERATIONS

A. Background Clearances

Condition: Critical contractor personnel, such as the RACF administrator and software

management personnel, did not have documented clearances.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies

to establish and manage personnel security policies, standards, and procedures that include requirements for screening individuals who: (1) participate in the design, development, operation, or maintenance of sensitive applications or (2) have access

to sensitive data.

Cause: While Federal employees are required to have background clearances, the Service

Center did not apply this requirement to contractors.

Effect: Without proper personnel screening, managers had limited knowledge of the

suitability of contractor personnel, from a security standpoint, for their respective jobs. Without this assurance, the risk is increased for the Service Center's sensitive

systems to be compromised.

Recommendation:

We recommend that the Director, Administrative Service Center, require all contractor employees to have the proper background clearances.

B. LAN Monitoring

Condition:

Four file servers at the Service Center had minimal lockout settings. For example, current lockout procedures provide for only a 15-minute lockout after three or four unsuccessful log-in attempts. We believe that these lockout settings would not adequately identify unauthorized access. The NetWare operating system software supports an "intruder detection/lockout feature," which aids in the prevention of unauthorized access to the system. The system will suspend a user account when a predefined number of unsuccessful access attempts occurs in a predetermined amount of time. The time that an account is suspended may also be defined.

Criteria:

The Privacy Act of 1974 and the Computer Security Act of 1987 require implementation of minimally acceptable security practices for improving the security and privacy of sensitive information in Federal computer systems. Office of Management and Budget Circular A-1 30 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Also, the Circular requires agencies to ensure that appropriate safeguards exist in general support systems (for example, LANs and the data processing center, including the operating system and utilities). In addition, industry standards recommend a lockout period of 7 days.

Cause:

Service Center officials stated that the 15-minute lockout met the Bureau of Reclamation's LAN standards. However, the Bureau's LAN implementation guidelines recognize that the minimum settings for intruder lockout parameters may be unacceptable to many offices. We believe, given the sensitivity of data at the Service Center, that minimum settings are unacceptable to ensure protection from unauthorized access to sensitive data.

Effect:

The minimum level of security set for the LAN increases the risk that unauthorized access to the Service Center's LAN resources will not be detected timely.

Recommendation:

We recommend that the Director, Administrative Service Center, enhance the intruder detection settings above the Bureau of Reclamation's policy to suspend a user account, after unsuccessful access attempts, for a period of time long enough to ensure that the user will have to contact an administrator to have the user ID reset. For example, the user ID could be suspended for 24 hours after three incorrect attempts occurred in a 24-hour period.

C. LAN Disaster Recovery Plan

Condition: The Service Center did not have a documented disaster recovery plan for its LAN.

This weakness was identified in a March 1994 Office of Inspector General audit report (No. 94-I357). The report recommended that the Service Center complete a risk analysis (the first step in developing a disaster recovery plan) on its LAN.

Criteria: Office of Management and Budget Circular A- 130, Appendix III, requires agencies

to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Specifically, agencies should establish a contingency plan and periodically test the capability of the

plan to perform the function in the event that its automated systems fail

Cause: Because no risk analysis has been performed on the LAN, no disaster recovery plan

has been developed by the Service Center.

Effect: The lack of a disaster recovery plan increases the risk that offices will not be able to

resume processing on a timely basis after a disaster occurs.

Recommendation:

We recommend that the Director, Administrative Service Center, develop and periodically update a disaster recovery plan for the LAN.

D. User Access Control

Condition:

The security settings that provide access to the file servers were not controlled. We identified weaknesses in the way user profiles had been established. In NetWare, established user profiles superseded the file server default restrictions. As such, some users had a required password change interval greater than 90 days, had concurrent multiple or unlimited connections, and were not required to use unique passwords.

In addition, the "SECURE CONSOLE" command was not used on any of the file servers we reviewed. The "SECURE CONSOLE" command is designed to prevent users from gaining access to the file server console by removing DOS from the system memory when the operating system is powered down. Also, the "SET ALLOW UNENCRYPTED PASSWORD = ON" was found on two of the file servers reviewed. This designation allows passwords to be UNENCRYPTED, thereby increasing the risk for passwords to be obtained and used by unauthorized users.

Criteria:

Office of Management and Budget Circular A- 130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems, It also requires agencies to implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The Circular further defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

Cause:

Service Center procedures were not followed or were not in place to ensure that controls were adequate to safeguard the LANs.

Effect:

The minimum security settings for the Service Center's LAN increase the risk for unauthorized access to network systems, which could result in the loss of data and in unauthorized individuals gaining access to sensitive data files through DOS by bringing down the file server.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Ensure that LAN security and password features are implemented, which will require all users to change passwords every 90 days, enforce unique password use, and limit concurrent multiple or unlimited connections to one per user and grant additional connections on an as-needed basis.
- 2. Include the "SECURE CONSOLE" command in the AUTOEXEC.NCF file on all file servers to prevent users from gaining access to the system files in DOS mode.
- 3. Ensure that the command "SET ALLOW UNENCRYPTED PASSWORD=ON" is not present in the AUTOEXEC.NCF file.

FFS APPLICATION

E. Access Security Controls

Condition: FFS security access controls were not adequate. We identified 15 users, who were

Service Center employees, who could update and modify the application vendor table of one of the Service Center's clients, as well as initiate disbursement documents. This access could result in the vendor table being changed and in an unauthorized

disbursing document being entered.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires that

security controls for personnel include such controls as individual accountability, "least privileged," and separation of duties. "Least privileged" is the practice of restricting users' access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, or delete) to the minimum necessary for the users to perform their jobs. Separation of duties is the practice of dividing the steps in a

critical function among different individuals.

Cause: Although the Service Center provided payment services to its client, the Service

Center had not ensured that security controls in the FFS application prevented unauthorized payments. Service Center officials stated that the client was responsible

for establishing the application security.

Effect: Without the applicable security access controls, the risk is increased for unauthorized

payments to be disbursed.

Recommendation:

We recommend that the Director, Administrative Service Center, coordinate with the client to limit Service Center users' access to the "least privileged" in the FFS application; that is, assurance should be provided that any user authorized to enter or change the vendor table does not also have access to disbursing documents.

F. Physical Security

Condition:

Although access to the Service Center facilities was controlled, the Service Center could not identify all individuals who had card key access to the computer rooms, which house the mainframe and LAN. In addition, some Service Center visitors (for example, maintenance personnel, janitorial staff, and vendors) were not monitored when they were inside the computer room.

Criteria:

The Department of the Interior Automated Information System Handbook, when addressing the control for personnel access to computer facilities, states, "Access by visitors, equipment personnel, and other individuals not directly involved with managing or operating a sensitive automated information system installation will be controlled by individual authorization." The Handbook further states that it is recognized that different procedures and restrictions will be required for various categories of visitors but that all access by other than assigned personnel will be monitored.

Cause:

The Service Center's informal procedures provided for vendors, as well as for the building management company, to be issued card keys to these sensitive areas without identifying the individuals receiving the cards and without requiring formal access request forms. Also, current practices allow certain visitors to be unmonitored when they are in the sensitive areas,

Effect:

The Service Center cannot specifically identify all those individuals who have access to and/or are accessing the computer rooms. Furthermore, by not monitoring all visitors, the risk is increased for the Service Center's sensitive data and resources to be stolen or destroyed.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Document procedures for the issuance of key cards and require that the procedures be instituted for vendors in addition to contractors and Federal employees.
- 2. Evaluate the need for individuals outside of the ADP Services Division to be issued permanent card keys because such access should be limited to those individuals performing their day-to-day duties.
- 3. Document procedures to ensure the Service Center's compliance with the Department of the Interior Automated Information Systems Handbook regarding visitor (such as maintenance personnel, janitorial staff, and vendors) monitoring.

G. Password Settings

Condition: In RACF, general client user passwords for access to the mainframe were not

prompted for change until after 180 days, and user ID codes were not automatically

revoked until 180 days of inactivity.

Criteria: The Department of the Interior Automated Information Systems Security Handbook

recommends that passwords be changed every 90 days. Also, generally accepted industry standards indicate that password change intervals should be from 60 to 90 days for users who do not have sensitive privileges and every 30 days for users who do have sensitive privileges because passwords may be guessed, copied, overheard,

or recorded and played back.

Cause: To make access to the mainframe applications more convenient for Service Center

clients who use the mainframe applications only occasionally, notably the SF-52 System users, the Service Center increased the password interval to 180 days in 1994 after receiving approval from the Bureau of Reclamation's Security Administrator. However, this approval recommended that the Service Center change the password parameters, such as requiring a numeric or special character as part of the password, set in RACF security software. Service Center officials stated that the 180-day interval was acceptable because of security available within the mainframe

applications. However, not all of the mainframe applications have access security.

Effect: The current password settings reduce the effectiveness of the password as a control, thereby increasing the risk for unauthorized access to sensitive information through

password disclosure.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Evaluate the feasibility of setting the parameters in RACF security software to require one numeric or special character as part of the password, as recommended by the Bureau of Reclamation's Security Administrator.
- 2. Reevaluate the standard RACF password change intervals and revocation settings to ensure that the level of risk associated with the mainframe applications and the current password settings is

acceptable to the Service Center, as well as to its clients and the Department, and address these results in a current risk assessment.

H. SMF Logs

Condition:

At least 27 Service Center user ID codes that were allowed access to the TSO software had "alter" access to the "SYS1.MAN%" dataset. The SYS1.MAN% dataset contains the SMF logs that record all system activity, thereby providing a system audit trail. In addition, a critical SMF record type, record type 60, was not active.

Criteria:

Office of Management and Budget Circular A-130 recommends that adequate audit trails exist so that an adverse impact on general support systems is prevented or detected. Also, Federal Information Processing Publication 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," provides guidelines for system security and addresses the importance of having audit trails of all system activity.

Cause:

The Service Center had insufficient policies and procedures surrounding the protection of the SYS1.MAN% datasets. Also, SMF record type 60 was not active because Service Center officials said that they believed another software product INFOPAC (report generation software) created too many records. They said, therefore, that to reduce the amount of storage needed for SMF logs, record type 60 was not activated.

Effect:

By allowing users "alter" access to these logs, the risk is increased for the SMF logs to be inaccurate. Furthermore, because record type 60 is not active, no system audit trail exists to determine whether the changes to sensitive datasets by authorized individuals are appropriate. Specifically, because the PAY/PERS application has no internal security to monitor access and changes to its datasets, the Service Center relies only on RACF security. The active SMF record types identified only security violations and did not record changes made to datasets. Therefore, in the PAY/PERS application, there was no system audit trail available to monitor and evaluate changes made to PAY/PERS sensitive data.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Evaluate the feasibility of limiting the number of Service Center users who have access authority to alter SMF logs.
- 2. Ensure that the SMF record type 60 logging is active or RACF settings are adjusted to specifically audit critical datasets maintained on the mainframe computers and to therefore provide an audit trail of system activity.

I. "OPERATIONS" Attribute

Condition:

The Service Center gave access to all of the operating system resources by assigning the "OPERATIONS" attribute to 85 active Service Center user IDs without logging the activities of these users. Through this access, users could make unauthorized changes to the mainframe computer operating system and sensitive application datasets without being detected by routine security controls.

Criteria:

The RACF Auditor's Guide states that "the OPERATIONS attribute allows a user access to almost all resources" and that the "group-OPERATIONS attribute allows a user access to almost all resources within the scope of the group and its subgroups." The "OPERATIONS" attribute, with some exceptions, provides the user with full control over datasets. Further, the RACF Security Administrator's Guide recommends that the "OPERATIONS" attribute be assigned to a minimum number of people and that the activities of the users be logged. RACF allows the use of more restrictive authorities, such as DASDVOL authority, when routine maintenance operations are performed. RACF security software also provides the option to log activities of users with the "OPERATIONS" attribute by activating the OPERAUDIT option.

Cause:

The Service Center had not assigned more restrictive authorities to individuals who performed routine system maintenance tasks because the Service Center had not evaluated the system access authority needed for individual users in performing their day-to-day functions. Also, the Service Center had not implemented the OPERAUDIT security feature in RACF that would log user activities as a result of the "OPERATIONS" attribute.

Effect:

Because the OPERAUDIT security feature had not been activated, any resource on the mainframe computer could be accessed using the "OPERATIONS" attribute without recording the user's access. This setting, along with the lack of system audit trails that would be produced by the SMF 60 record type, increases the risk for intentional or accidental unauthorized system actions to occur and not be detected.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Evaluate the extent to which the "OPERATIONS" attribute should be available to Service Center user IDs. Specifically, the use of other more restrictive RACF authorities (such as DASDVOL authority) should be considered where possible.
- 2. Activate the security feature RACF OPERAUDIT and ensure that security personnel perform periodic reviews of the resultant logs to identify unauthorized activity.

J. ADP Access Levels

Condition: Users in the Service Center's ADP Services Division had significant access levels.

For example, 28 user IDs had RACF authority to emulate the master console, even though the authority to issue operator commands through the TSO was not given to these individuals. In addition, 28 user IDs had "alter" access to the system parameter

libraries (for example, the SYS1.PARMLIB) through the TSO.

Criteria: Office of Management and Budget Circular A-130 requires, at a minimum, that

agency programs incorporate controls such as "separation of duties, least privileged,

and individual accountability" within their major applications.

Cause: Because of other Service Center priorities, the group responsible for monitoring

security had not performed an audit of user access levels and therefore had not identified the required necessary changes and had not ensured that user access was at the authorized level. In addition, the ADP Services Division had not implemented procedures to ensure that "least privileged" access controls and appropriate separation

of duties were in place.

Effect: By allowing significant access levels to critical functions, the risk is increased for

datasets to be altered without authorization and for the alteration to go undetected by normal operating controls. Without periodic review of user access levels, the risk is increased that the access given to a user will exceed that which is necessary to

perform the user's daily job.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Ensure that the group responsible for monitoring security performs periodic reviews of user access levels to identify required necessary changes and to ensure that user access levels are authorized.
- 2. Institute a policy of "least privileged" access levels to ensure that access to resources and data is limited to those users who require such access.

K. RACF Software Internal Controls

Condition: Responsibilities of the RACF security administrator (assigned the SPECIAL attribute

within RACF) had been combined with the responsibilities of the RACF auditor (assigned the AUDITOR attribute within RACF). In addition, seven user IDs within the Service Center had these combined attributes. This weakness was previously identified in a March 1994 Office of Inspector General audit report (No. 94-I-357).

Criteria: The RACF Auditor's Guide addresses the importance of the separation of duties

between the security administrator and the auditor. The Guide states, "The separation of powers is necessary because it is the security administrator's job to establish RACF controls, and it is the auditor's function to test the adequacy and effectiveness of these

controls. "

Cause: Service Center officials stated that RACF security administrator and RACF auditor

functions were performed by the same individual because of the limited number of staff assigned to the group responsible for monitoring security. They further stated that the Service Center had a limited number of individuals who had expertise in the

area of RACF administration,

Effect: The control over the RACF security administrator function is lost because there was

no systematic monitoring of this powerful function. Therefore, the risk exists for accidental or intentional unauthorized actions that could disrupt information system

operations and threaten the integrity of the sensitive information.

Recommendation:

We recommend that the Director, Administrative Service Center, evaluate the staffing requirements of the group responsible for monitoring security to ensure the separation of duties within RACF.

L. Authorization - Internal Controls

Condition: Mainframe access given to users as assigned in RACF was not always supported by

a formal request or was not recorded in the Service Center's Decentralized Security

Administration Facility.

Criteria: The Service Center's policy is for formal authorization requests to be obtained from

the designated security point of contact before users are permitted to access sensitive data on the mainframe computer. In addition, the point of contact can orally notify the Service Center for adjustments to the users' access requirements. Also, generally accepted industry standards recommend that reconciliations exist between what has been formally requested and what access level was actually granted to ensure that

mishandling, alterations, and misunderstandings are reduced.

Cause: Orally requested access level adjustments that were approved were not always

recorded in the access request system because the Service Center did not always

enforce the procedures to record approved access level adjustments.

Effect: By not updating Decentralized Security Administration Facility records for

adjustments to accesses requested, the system administrator cannot reconcile the formal authorization and the Decentralized Security Administration Facility records with the RACF access levels assigned to users and thus ensure that access is assigned

at the appropriate level.

Recommendation:

We recommend that the Director, Administrative Service Center, document and implement procedures to ensure that Decentralized Security Administration Facility records are updated for oral access adjustments to allow for the reconciliation of access requested with access allowed.

M. Computer Security Plan/Report

Condition: The Service Center had not developed a security plan for fiscal year 1996

Criteria: The Computer Security Act of 1987 requires that all agencies improve the security

and privacy of sensitive information in Federal computer systems. Specifically, the Act requires that security plans be developed for all sensitive computer systems. A computer security plan is designed to assist agencies in addressing the protection of general support systems and major applications that contain sensitive information to help ensure the system's integrity, availability, and confidentiality. In addition, Office of Management and Budget Circular A-130, Appendix III, states that agencies without adequate security plans should consider classifying this as a material weakness in their annual Federal Managers' Financial Integrity Act report to the

Congress.

Cause: A computer security plan was not prepared for fiscal year 1996 because of limited

staffing in the group responsible for monitoring security.

Effect: Without this plan, the Service Center did not have adequate assurance that data in its

sensitive systems were adequately protected. In addition, the Service Center had a material weakness, which should be reported in its annual Federal Managers' Financial

Integrity Act report to the Congress.

Recommendation:

We recommend that the Director, Administrative Service Center, provide resources to ensure the development of a computer security plan for the sensitive systems in accordance with the Computer Security Act and Circular A-130, Appendix III.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

N. Continuity of Operations Plan

Condition: The Service C

The Service Center's Continuity of Operations Plan (dated December 28,1995) did not address recovery of one of the sensitive systems, the FFS; the LAN; and critical telecommunications links. Also, the Plan had not been updated to reflect all tests of the Plan completed in 1996. Additionally, the risk analysis, upon which the Plan is to be based, had not been updated since July 1990.

Criteria:

Office of Management and Budget Circular A- 130 requires agencies to establish a comprehensive contingency plan and periodically test the capability to perform the agency function supported by the application, as well as critical telecommunications links, in the event of a disaster or system failure. In order to accurately and successfully test the disaster recovery capabilities, the disaster recovery plans need to be updated as changes occur. In addition, the Circular states that "manual procedures are generally NOT [emphasis in original] a viable back-up option."

Cause:

Service Center officials said that update of the risk analysis and continuity of operations plan had low priorities. In addition, Service Center officials stated that the FFS application was not included in the Plan as a result of Service Center clients agreeing that FFS services could be delayed for 30 days because processing could be performed manually. However, we found no documentation of such agreements.

Effect:

If the Continuity of Operations Plan is incorrect (such as by not including all sensitive systems) or is outdated, personnel required to perform the disaster recovery procedures may not be able to recover critical systems in the event of a disaster or system failure.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Perform a risk analysis of the Service Center's computer center and its applications.
- 2. Update the existing Continuity of Operations Plan for the mainframe, sensitive applications, and telecommunications links so that the current operating environment is documented.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

O. Comprehensive Business Recovery Plan

Condition: No comprehensive business recovery plan had been developed for the Service Center.

The only plan in existence at the Service Center was the Continuity of Operations Plan, which addressed only the recovery of the systems environment. The Plan did not address business and user operations that need to be in effect for the Service

Center to support its clients in the event of a disaster or system failure.

Criteria: Office of Management and Budget Circular A-1 30 requires agencies to establish

controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, generally accepted information systems standards recognize that a comprehensive business recovery plan is necessary to ensure the timely recovery of all business functions and of the systems environment, both of which are critical for day-to-day operations, and to minimize

down time.

Cause: The Service Center's emphasis was on the restoration of the mainframe environment

rather than on the recovery of business operations.

Effect: If a disaster or system failure occurs, the Service Center may not be able to recover

all business functions and systems necessary for the continued long-term operations

of the organization.

Recommendation:

We recommend that the Director, Administrative Service Center, develop a comprehensive business recovery plan, which includes procedures for its business functions.



United States Department of the Interior

BUREAU OF RECLAMATION

Washington. D.C. 20240

MAR 2 4 1997

D-5010 ADM-8.00

MEMORANDUM

To: Office of Inspector General

Attention: Acting Assistant Inspector General for Audits

From: Eluid L. Martinez

Commissioner

Subject: Draft Audit Report on Mainframe Computer Policies and Procedures

(Assignment No. A-IN-BOR-001-96)

The Bureau of Reclamation appreciates the opportunity to comment on the subject report. Reclamation concurs or has complied with 23 of the 24 of the audit recommendations and we fully recognize the importance of computer security and that our policies and procedures can be improved. However, we believe the Administrative Service Center (ASC) has in place an adequate security program and are concerned with certain aspects of the report as outlined below.

The report identified physical security as a weakness, We believe extensive physical security measures are in place at the ASC. The computer and related hardware (such as mainframe computer, direct access storage devices, tape devices, telecommunications equipment, large volume printers, etc.) are located in a locked computer room controlled for authorized access only. In addition, the computer room is located in a secure building where all outside doors are locked and require an individual access card for authorized entry. ASC security also includes on-site armed guard service 24 hours a day, 7 days a week. Following the Oklahoma City bombing, the Justice Department was directed by the President to conduct a Vulnerability Assessment of Federal Facilities. This assessment recognized five levels of security for Federal facilities based upon perceived threat and established security standards for each of the live levels. Based on this criteria, the ASC was deemed a Level III facility. The GSA participated in a review of ASC security and concluded the ASC exceeded Level III security requirements.

The audit report identified areas to reduce security risks and recommended specific actions to reduce those risks. Both OMB Circulars A-123 and A-130 recognize cost as an important consideration and require that agencies implement cost effective management and internal controls. For instance, OMB Circular A-130 recognizes both risk and cost in addressing "adequate security." Yet, discussions with the auditors confirmed that cost was not considered in recommending these specific actions to reduce risk.

2

The audit report referred to "generally accepted industry and information systems standards" and reported the ASC as noncompliant in several instances. Discussions with the auditors confirmed that a conclusive set of these "standards" was not available and the auditors were not aware as to whether these "standards" had ever been issued as official Government-wide policy. The Department of the Interior's Office of Information Resources Management likewise advised that they were unaware of these "standards" and their applicability to Interior organizations.

Again, we appreciate the opportunity to comment on the subject report. Attached are our specific comments for each recommendation. If you have any questions or require additional information, please contact Luis Maez at (303) 236-3289, extension 245.

Attachment

cc: Assistant Secretary - Water and Science, Attention: Margaret Carpenter (w/attachment)

COMPUTER CENTER MANAGEMENT AND OPERATIONS

A. Background Clearances

Condition: Critical contractor personnel, such as the RACF administrator and software

management personnel, did not have documented clearances.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies

to establish and manage personnel security policies, standards, and procedures that include requirements for screening individuals who: (1) participate in the design, development, operation, or maintenance of sensitive applications or (2) have access

to sensitive data.

Cause: While Federal employees are required to have background clearances, the Service

Center did not apply this requirement to contractors.

Effect: Without proper personnel screening, managers had limited knowledge of the

suitability of contractor personnel, from a security standpoint, for their respective jobs. Without this assurance, the risk is increased for the Service Center's sensitive

systems to be compromised.

Recommendation

We recommend that the Director, Administrative Service Center, require all contractor employees to have the proper background clearances.

Response

Complied. All ADP contractor employees, including RACF administrators and systems software management personnel, are required to have background clearances. The Statement of Work for the GSA Tri-Part Contract (which ADP Services Division uses) contained a Level 3, critical-sensitive requirement, but this provision was not previously enforced. Also, at our request, the Colorado Bureau of Investigation has completed background investigations on all ADP contractor personnel. This is also a continuing requirement for all new-hire contractor personnel.

B. LAN Monitoring

Condition:

Four file servers at the Service Center had minimal lockout settings. For example, current lockout procedures provide for only a 15-minute lockout after three or four unsuccessful log-in attempts. We believe that these lockout settings would not adequately identify unauthorized access. The NetWare operating system software supports an "intruder detection/lockout feature," which aids in the prevention of unauthorized access to the system. The system will suspend a user account when a predefined number of unsuccessful access attempts occurs in a predetermined amount of time. The time that an account is suspended may also be defined.

Criteria:

The Privacy Act of 1974 and the Computer Security Act of 1987 require implementation of minimally acceptable security practices for improving the security and privacy of sensitive information in Federal computer systems. Office of Management and Budget Circular A-130 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Also, the Circular requires agencies to ensure that appropriate safeguards exist in general support systems (for example, LANs and the data processing center, including the operating system and utilities). In addition, industry standards recommend a lockout period of 7 days.

Cause:

Service Center officials stated that the 15-minute lockout met the Bureau of Reclamation's LAN standards. However, the Bureau's LAN implementation guidelines recognize that the minimum settings for intruder lockout parameters may be unacceptable to many offices. We believe, given the sensitivity of data at the Service Center, that minimum settings are unacceptable to ensure protection from unauthorized access to sensitive data.

Effect:

The minimum level of security set for the LAN increases the risk that unauthorized access to the Service Center's LAN resources will not be detected timely.

Recommendation

We recommend that the Director, Administrative Service Center, enhance the intruder detection settings above the Bureau of Reclamation's policy to suspend a user account, after unsuccessful access attempts, for a period of time long enough to ensure that the user will have to contact an administrator to have the user ID reset. For example, the user ID could be suspended for 24 hours after three incorrect attempts occurred in a 24-hour period.

Response

Concur with intent. Although lockout settings already meet Reclamation LAN standards, we are willing to consider additional security enhancements as deemed appropriate. An evaluation will be made to determine if the settings should **be** changed. This evaluation is scheduled to be completed by June 30, 1997. The responsible official is the Chief, ADP Services Division.

C. LAN Disaster Recovery Plan

Condition: The Service Center did not have a documented disaster recovery plan for its LAN.

This weakness was identified in a March 1994 Office of Inspector General audit report (No. 94-I357). The report recommended that the Service Center complete a risk analysis (the first step in developing a disaster recovery plan) on its LAN.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies

to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Specifically, agencies should establish a contingency plan and periodically test the capability of the

plan to perform the function in the event that its automated systems fail.

Cause: Because no risk analysis has been performed on the LAN, no disaster recovery plan

has been developed by the Service Center.

Effect: The lack of a disaster recovery plan increases the risk that offices will not be able to

resume processing on a timely basis after a disaster occurs.

Recommendation

We recommend that the Director, Administrative Service Center, develop and periodically update a disaster recovery plan for the LAN.

Response

Concur. A risk analysis of the ASC LAN environment will be completed by September 30, 1997. The risk analysis will provide the basis for development of a LAN Disaster Recovery Plan which is targeted for completion by March 3 1, 1998. The responsible official is the Chief, ADP Services Division.

D. User Access Control

Condition:

The security settings that provide access to the file servers were not controlled. We identified weaknesses in the way user profiles had been established. In NetWare, established user profiles superseded the file server default restrictions. As such, some users had a required password change interval greater than 90 days, had concurrent multiple or unlimited connections, and were not required to use unique passwords.

In addition, the "SECURE CONSOLE" command was not used on any of the file servers we reviewed. The "SECURE CONSOLE" command is designed to prevent users from gaining access to the file server console by removing DOS from the system memory when the operating system is powered down. Also, the "SET ALLOW UNENCRYPTED PASSWORD = ON" was found on two of the file servers reviewed. This designation allows passwords to be UNENCRYPTED, thereby increasing the risk for passwords to be obtained and used by unauthorized users.

Criteria:

Office of Management and Budget Circular A- 130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. It also requires agencies to implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The Circular further defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. "

Cause:

Service Center procedures were not followed or were not in place to ensure that controls were adequate to safeguard the LANs.

Effect:

The minimum security settings for the Service Center's LAN increase the risk for unauthorized access to network systems, which could result in the loss of data and in unauthorized individuals gaining access to sensitive data files through DOS by bringing down the file server.

LAN PROTECTION

Recommendations

We recommend that the Director, Administrative Service Center:

1. Ensure that LAN security and password features are implemented, which will require all users to change passwords every 90 days; enforce unique password use; and limit concurrent multiple or unlimited connections to one per user and grant additional connections on an as-needed basis.

Response

Complied. The password change interval has been changed to 90 days or less on all servers. Unique passwords are now required for all individual users. Concurrent multiple connection authority has been removed from all accounts with the exception of those where a demonstrated need. exists. Requests for multiple concurrent connections now require completion of an ASC-14 Computer Security Access Request Form with appropriate supervisory authorization.

2. Include the "SECURE CONSOLE" command in the AUTOEXEC.NCF file on all file servers to prevent users from gaining access to the system files in DOS mode.

Response

Complied. A procedure to secure the console on all ASC file servers was implemented in August 1996. The "LOAD MONITOR" command with the "lock" option was included in the AUTOEXEC.NCF file in January 1997.

3. Ensure that the command "SET ALLOW UNENCRYPTED PASSWORD=ON" is not present in the AUTOEXEC.NCF file.

Response

Concur. The "SET ALLOW UNENCRYPTED PASSWORD=ON" command cannot be set at this time. Certain versions of the NETWARE "NETX" client requestor are present on some ASC workstations that are not compliant with the encrypted password feature. When the migration to Netware 4. lx NDS (Novell Directory Services) is completed at the ASC and all client workstations have been migrated to Netware VLMs, this command will be invoked on all file servers. Migration to NDS will be completed as part of a Reclamation-wide effort. Although unencrypted passwords are accepted at this time, the vast majority of passwords processed by ASC file servers are currently encrypted. Target date for completion is March 3 1, 1998. The responsible official is the Chief, ADP Services Division.

FFS APPLICATION

E. Access Security Controls

Condition: FFS security access controls were not adequate. We identified 15 users. who were

Service Center employees. who could update and modify the application vendor table of one of the Service Center's clients, as well as initiate disbursement documents. This access could result in the vendor table being changed and in an unauthorized

disbursing document being entered.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires that

security controls for personnel include such controls as individual accountability, "least privileged," and separation of duties. "Least privileged" is the practice of restricting users' access (to **data** files, to processing capability, or to peripherals) or type of access (read, write, execute, or delete) to the minimum necessary for the users to perform their jobs. Separation of duties is the practice of dividing the steps in a

critical function among different individuals.

Cause: Although the Service Center provided payment services to its client, the Service

Center had not ensured that security controls in the FFS application prevented

unauthorized payments.

Effect: Without the applicable security access controls, the risk is increased for unauthorized

payments to be disbursed.

Recommendation

We recommend that the Director, Administrative Service Center. coordinate with the client to limit Service Center users' access to the "least privileged" in the FFS application; that is, assurance should be provided that any user authorized to enter or change the vendor table does not also have access to disbursing documents.

Response

Complied. As requested by the ASC, the client has changed FFS security such that no employees have access to both the vendor tables and disbursement function. It should be noted that this condition was confined strictly to the transfer of a client's administrative payments function and related employees to the ASC in May 1996. The client is responsible for managing and controlling FFS access for this payments function. In other words, the ASC cannot initiate or change FFS access for employees performing this client's payments. Also, it should be noted that discussions with the auditors confirmed that no unauthorized disbursements were found.

F. Physical Security

Condition:

Although access to the Service Center facilities was controlled, the Service Center could not identify all individuals who had card key access to the computer rooms, which house the mainframe and LAN. In addition, some Service Center visitors (for example, maintenance personnel, janitorial staff, and vendors) were not monitored when they were inside the computer room.

Criteria:

The Department of the Interior Automated Information System Handbook, when addressing the control for personnel access to computer facilities, states, "Access by visitors, equipment personnel, and other individuals not directly involved with managing or operating a sensitive automated information system installation will be controlled by individual authorization." The Handbook further states that it is recognized that different procedures and restrictions will be required for various categories of visitors but that all access by other than assigned personnel will be monitored.

Cause:

The Service Center's informal procedures provided for vendors, as well as for the building management company, to be issued card keys to these sensitive areas without identifying the individuals receiving the cards and without requiring formal access request forms. Also, current practices allow certain visitors to be unmonitored when they are in the sensitive areas.

Effect:

The Service Center cannot specifically identify all those individuals who have access to and/or are accessing the computer rooms. Furthermore, by not monitoring all visitors, the risk is increased for the Service Center's sensitive data and resources to be stolen or destroyed.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Document procedures for the issuance of key cards and require that the procedures be instituted for vendors in addition to contractors and Federal employees.

Response

Complied. Procedures for the issuance of card keys for vendors, contractors, and Federal employees have been documented. As evidenced by this recommendation and Recommendation 3 (below), we believe this condition should have been more

appropriately **stated** as a currency of documentation issue. Two levels of security control must be passed before entry into the computer room. As concluded by GSA, ASC's physical security exceeds security standards for a Level III Federal facility. Although the ASC has always had a strong physical security emphasis and program in place, it was recently enhanced with implementation of a picture identification card system that is now compatible with the Bureau of Reclamation system for Building 67 at the Denver Federal Center.

2. Evaluate the need for individuals outside of the ADP Services Division to be issued permanent card keys because such access should be limited to those individuals performing their day-to-day duties.

Response

Complied. The evaluation was completed by the ADP Services Division and the Management Services Division in February 1997. Permanent card keys are issued to just those individuals deemed appropriate.

3. Document procedures to ensure the Service Center's compliance with the Department of the Interior Automated Information Systems Handbook regarding visitor (such as maintenance personnel, janitorial staff, and vendors) monitoring.

Response

Complied. Procedures for monitoring visitor access to the computer room have been documented by the Management Services Division in compliance with the Department of the Interior's Automated Information Systems Handbook.



G. Password Settings

Condition: In RACF, general client user passwords for access to the mainframe were not

prompted for change until after 180 days, and user ID codes were not automatically

revoked until 180 days of inactivity.

Criteria: The Department of the Interior Automated Information Systems Security Handbook

recommends that passwords be changed every 90 days. Also, generally accepted industry standards indicate that password change intervals should be from 60 to 90 days for users who do not have sensitive privileges and every 30 days for users who do have sensitive privileges because passwords may be guessed, copied, overheard,

or recorded and played back.

Cause: To make access to the mainframe applications more convenient for Service Center

clients who use the mainframe applications only occasionally, notably the SF-52 System users, the Service Center increased the password interval to 180 days in 1994 after receiving approval from the Bureau of Reclamation's Security Administrator. However, this approval recommended that the Service Center change the password parameters, such as requiring a numeric or special character as part of the password, set in RACF security software. Service Center officials stated that the 180-day in the mainframe

applications. However, not all of the mainframe applications have access security.

Effect: The current password settings reduce the effectiveness of the password as a control,

thereby increasing the risk for unauthorized access to sensitive information through

password disclosure.

Recommendations

We recommend that the Director. Administrative Service Center:

1. Evaluate the feasibility of setting the parameters in RACF security software to require one numeric or special character as part of the password, as recommended by the Bureau of Reclamation's Security Administrator.

Response

Concur. An evaluation of using one numeric or special character as part of the ASC standard password will be completed by September 30, 1997. The responsible official is the Chief, ADP Services Division.

2. Reevaluate the standard RACF password change intervals and revocation settings to ensure that the level of risk associated with the mainframe applications and the current password settings is acceptable to the Service Center, as well as to its clients and the Department, and address these results in a current risk assessment.

Response

Concur with intent. The ASC plans to reconfirm the 180-day interval with clients and the Department System Owner. This effort is targeted for completion September 30, 1997. The responsible official is the Chief, ADP Services Division.

It should be noted, however, that the 180-day password interval exists for only one application....the automated SF-52 System. The extended interval was requested by clients primarily for infrequent users of the system and was coordinated with the Department of the Interior System Owner and the Interior Department's Office of Information Resource Management. In addition a waiver to use the 1 80-day interval was obtained from the Bureau of Reclamation Computer Security Manager per the procedures set forth in 375 DM 19. It should also be noted that while 180 days is the overall system maximum, the password expiration period for each user is set individually by the client's Security Point-of-Contact based on their evaluation of the risk associated with the user. The ASC has issued guidance to its clients recommending that the expiration period of 180 days only be used for infrequent users of the system whose access presents a low risk. Finally, the last two sentences of the "Cause:" refer to mainframe applications and whether or not they have access security. Since the 180-day interval only relates to the automated SF-52 System which does have access security, the two sentences are not relevant to this issue.

H. SMF Logs

Condition:

At least 27 Service Center user ID codes that were allowed access to the TSO software had "alter" access to the "SYS1.MAN%" dataset. The SYS1.MAN% dataset contains the SMF logs that record all system activity. thereby providing a system audit trail. In addition a critical SMF record type, record type 60, was not active.

Criteria:

Office of Management and Budget Circular A-130 recommends that adequate audit trails exist so that an adverse impact on general support systems is prevented or detected. Also, Federal Information Processing Publication 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," provides guidelines for system security and addresses the importance of having audit trails of ail system activity.

Cause:

The Service Center had insufficient policies and procedures surrounding the protection of the SYS1.MAN% datasets. Also, SMF record type 60 was not active because Service Center officials said that they believed another software product INFOPAC (report generation software) created too many records. They said, therefore, that to reduce the amount of storage needed for SMF logs, record type 60 was not activated.

Effect:

By allowing users "alter" access to these logs, the risk is increased for the SMF logs to be inaccurate. Furthermore, because record type 60 is not active, no system audit trail exists to determine whether the changes to sensitive datasets by authorized individuals are appropriate. Specifically, because the PAY/PERS application has no internal security to monitor access and 'changes to its datasets, the Service Ctnter relies only on RACF security. The active SMF record types identified only security violations and did not record changes made to datasets. Therefore, in the PAY/PERS application, there was no system audit trail available to monitor and evaluate changes made to PAY/PERS sensitive data.

Recommendations

We recommend that the Director. Administrative Service Center:

1. Evaluate the feasibility of limiting the number of Service Center users who have access authority to alter SMF logs.

Response

Complied. The evaluation was completed in December 1996 to limit the number of individuals with access authority to alter SAF logs. This authority has now been limited to just three senior level system programmers that reside in the System Software Management Branch. The evaluation was completed by the Chief, Systems Management Branch, the ASC Computer Security Manager and approved by the Chief, ADP Services Division.

2. Ensure that the SMF record type 60 logging is active or RACF settings are adjusted to specifically audit critical **datasets** maintained on the mainframe computers and to therefore provide an audit trail of system activity.

Response

Complied. Batch and TSO type 60 records have always been written to the SMF log. Type 60 record collection has now been activated for "started tasks" as well.



I. "OPERATIONS" Attribute

Condition:

The Service Center gave access to all of the operating system resources by assigning the "OPERATIONS" attribute to 85 active Service Center user **IDs** without logging the activities of these users. Through this access, users could make unauthorized changes to the mainframe computer operating system and sensitive application datasets without being detected by routine security controls.

Criteria:

The RACF Auditor's Guide states that "the OPERATIONS attribute allows a user access to almost all resources" and that the "group-OPERATIONS attribute allows a user access to almost all resources within the scope of the group and its subgroups." The "OPERATIONS" attribute, with some exceptions, provides the user with full control over datasets. Further, the RACF Security Administrator's Guide recommends that the "OPERATIONS" attribute be assigned to a minimum number of people and that the activities of the users be logged. RACF allows the use of more restrictive authorities, such as DASDVOL authority, when routine maintenance operations are performed. RACF security software also provides the option to log activities of users with the "OPERATIONS" attribute by activating the OPERAUDIT option.

Cause:,

The Service Center had not assigned more restrictive authorities to individuals who performed routine system maintenance tasks because the Service Center had not evaluated the system access authority needed for individual users in performing their day-to-day functions. Also, the Service Center had not implemented the OPERAUDIT security feature in RACF that would log user activities as a result of the "OPERATIONS" attribute.

Effect:

Because the OPERAUDIT security feature had not been activated, any resource on the mainframe computer could be accessed using the "OPERATIONS" attribute without recording the user's access. This setting, along with the lack of system audit trails that would be produced by the SMF 60 record type, increases the risk for intentional or accidental unauthorized system actions to occur and not be detected.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Evaluate the extent to which the "OPERATIONS" attribute should be available to Service Center user IDs. Specifically, the use of other more restrictive RACF authorities (such as DASDVOL authority) should be considered where possible.

Response

Concur. An evaluation will be conducted to limit the "OPERATIONS" attribute to those authorized ADP personnel deemed necessary and appropriate as well as consider other more restrictive RACF authorities. Target date for completion is December 31, 1997. The responsible official is the Chief, ADP Services Division.

2. Activate the security feature RACF OPERAUDIT and ensure that security personnel perform periodic reviews of the resultant logs to identify unauthorized activity.

Response

Complied. The feature RACFOPERAUDIT has been activated and the resultantlogs will be reviewed on a quarterly basis by the ASC Computer Security Manager. It should be noted that this situation is restricted to ADP authorized personnel only.

J. ADP Access Levels

Condition: Users in the Service Center's ADP Services Division had significant access levels.

For example, 28 user IDs had RACF authority to emulate the master console, even though the authority to issue operator commands through the TSO was not given to these individuals. In addition 28 user IDs had "alter" access to the system parameter

libraries (for example, the SYS1.PARMLIB) through the TSO.

Criteria: Office of Management and Budget Circular A-130 requires, at a minimum, that

agency programs incorporate controls such as "separation of duties, least privileged,

and individual accountability" within their major applications.

Cause: Because of other Service Center priorities. the group responsible for monitoring

security had not performed an audit of user access levels and therefore had not identified the required necessary changes and had not ensured that user access was at the authorized level. In addition, the ADP Services Division had not implemented procedures to ensure that "least privileged" access controls and appropriate separation

procedures to ensure that "least privileged" access controls and appropriate separation

of duties were in place.

Effect: By allowing significant access levels to critical functions, the risk is increased for

datasets to be altered without authorization and for the alteration to go undetected by normal operating controls. Without periodic review of user access levels, the risk is increased that the access given to a user will exceed that which is necessary to

perform the user's daily job.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Ensure that the group responsible for monitoring security performs periodic reviews of user access levels to identify required necessary changes and to ensure that user access levels are authorized.

Response

Concur. A project to identify and initialize auditing for all critical sensitive datasets will be started. The target date for completion is June 30, 1997. The responsible official is Chief, ADP Services Division.

2. Institute a policy of "least privileged" access levels to ensure that access to resources and data is limited to those users who require such access.

Response

Complied. A policy of "least privileged" access is now in place. While the capability to emulate the master console is assigned to a few individuals, the ability to issue critical operating system level commands has not been given. These commands are limited to the master console which is located in a locked, secured computer room accessible by authorized personnel only.

K. RACF Software Internal Controls

Condition:

Responsibilities of the RACF security administrator (assigned the SPECIAL attribute within RACF) had been combined with the responsibilities of the RACF auditor (assigned the AUDITOR attribute within RACF). In addition, seven user **IDs** within the Service Center had these combined attributes. This weakness was previously identified in a March 1994 Office of Inspector General audit report (No. 94-I-357).

Criteria:

The RACF Auditor's Guide addresses the importance of the separation of duties between the security administrator and the auditor. The Guide states, "The separation of powers is necessary because it is the security administrator's job to establish RACF controls, and it is the auditor's function to test the adequacy and effectiveness of these controls."

Cause:

Service Center officials **stated** that RACF security administrator and RACE-auditor functions were performed by the same individual because of the limited number of staff assigned to the group responsible for monitoring security. They further stated that the Service Center had a limited number of individuals who had expertise in the area of RACF administration.

Effect:

The control over the RACF security administrator function is lost because there was no systematic monitoring of this powerful function. Therefore, the risk exists for accidental or intentional unauthorized actions that could disrupt information system operations and threaten the integrity of the sensitive information.

Recommendation

We recommend that the Director, Administrative Service Center, evaluate the staffing requirements of the group responsible for monitoring security to ensure the separation of duties within RACF.

Response

Concur. Staffing requirements will be evaluated to ensure the separation of duties within RACF. Separation of RACF administrator and auditor responsibilities will be accomplished to the maximum extent possible. However, combining these responsibilities in isolated situations is necessary and will be managed accordingly. Also, we disagree with the statement that this condition was caused by "the limited number of staff assigned to the group responsible for monitoring security." This information does not represent the ASC position. The target date for completion of this evaluation is September 30, 1997. The responsible official is the Chief, ADP Services Division.

L. Authorization - Internal Controls

Condition: Mainframe access given to users as assigned in RACF was not always supported by

a formal request or was not recorded in the Service Center's Decentralized Security

Administration Facility.

Criteria: The Service Center's policy is for formal authorization requests to be obtained from

the designated security point of contact before users are permitted to access sensitive **data on** the mainframe computer. In addition, the point of contact can orally notify the Service Center for adjustments to the users' access requirements. Also, generally accepted industry standards recommend that reconciliations exist between what has been formally requested and what access level was actually granted to ensure that

mishandling, alterations, and misunderstandings are reduced.

Cause: Orally requested access level adjustments that were approved were not always

recorded in the access request system because the Service Center did not always

enforce the procedures to record approved access level adjustments.

Effect: By not updating Decentralized Security Administration Facility records for

adjustments to accesses requested, the system administrator cannot reconcile the formal authorization and the Decentralized Security Administration Facility records with the RACF access levels assigned to users and thus ensure that access is assigned

at the appropriate level.

Recommendation

We recommend that the Director, Administrative Service Center, document and implement procedures to ensure that Decentralized Security Administration Facility records are updated for oral access adjustments to allow for the reconciliation of access requested with access allowed.

Response

Nonconcur. We disagree there is a problem and question any adverse effect. Formal requests for user access are made through client Security Points-of-Contact to the ASC Security Manager. As users begin accessing the system revisions to their access are sometimes necessary in order to perform their duties. To expedite these revisions, client Security Points-of-Contact may orally contact the ASC Security Manager. Since only client and ASC security officials can effect these access revisions, we

question any adverse effect as well as any benefit from retroactively requiring additional documentation. Also, "generally accepted industry standards" are cited as applicable criteria. As previously addressed in our response, discussions with the auditors confirmed that a conclusive set of "generally accepted industry and information system standards" were not available and the auditors were not aware as to whether these "standards" had ever been issued as official Government-wide policy. The Department of the Interior's Office of Information Resources Management likewise advised that they were unaware of these "standards" and their applicability to Interior organizations. Finally, we question the recommendation in terms of consistency with OMB policies. Both OMB Circulars A-123 and A-130 recognize cost as an important consideration and require that agencies implement cost effective management and internal controls. For instance, OMB Circular A-130 recognizes both risk and cost in addressing "adequate security." Yet, discussions with the auditors confirmed that cost was not considered.

Same and the

M. Computer Security Plan/Report

Condition: The Service Center had not developed a security plan for fiscal year 1996.

Criteria: The Computer Security Act of 1987 requires that all agencies improve the security

and privacy of sensitive information in Federal computer systems. Specifically, the Act requires that security plans be developed for all sensitive computer systems. A computer security plan is designed to assist agencies in addressing the protection of general support systems and major applications that contain sensitive information to help ensure the system's integrity, availability, and confidentiality. In addition Office of Management and Budget Circular A-130, Appendix III, states that agencies without adequate security plans should consider classifying this as a material weakness in their annual Federal Managers' Financial Integrity Act report to the

Congress"

Cause: A computer security plan was not prepared for fiscal year 1996 because of limited

staffing in the group responsible for monitoring security.

Effect: Without this plan the Service Center did not have adequate assurance that data in its

sensitive systems were adequately protected. In addition, the Service Center had a material weakness, which should be reported in its annual Federal Managers' Financial

Integrity Act report to the Congress.

Recommendation

We recommend that the Director. Administrative Service Center, provide resources to ensure the development of a computer security plan for the sensitive systems in accordance with the Computer Security Act and Circular A-130, Appendix III. Also, the lack of a security plan should be reported as a material weakness to the Department of the Interior for inclusion in its next annual Federal Managers' Financial Integrity Act report until a plan is developed and meets the requirements of Circular A- 130.

Response

Complied. A current computer security plan was documented and submitted in January 1997 in accordance with Department of the Interior Office of Information Resources Management requirements. The ASC has had an effective security program in place that has included, for example, periodic reviews of security controls in each major system as required by OMB Circular A-130. These reviews have disclosed no significant security problems or deficiencies.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

N. Continuity of Operations Plan

Condition:

The Service Center's Continuity of Operations Plan (dated December 28,1995) did not address recovery of one of the sensitive systems, the FFS; the LAN; and critical telecommunications links. Also, the Plan had not been updated to reflect all tests of the Plan completed in 1996. Additionally, the risk analysis, upon which the Plan is to be based, had not been updated since July 1990.

Criteria:

Office of Management and Budget Circular A-130 requires agencies to establish a comprehensive contingency plan and periodically test the capability to perform the agency function supported by the application, as well as critical telecommunications links, in the event of a disaster or system failure. In order to accurately and successfully test the disaster recovery capabilities, the disaster recovery plans need to be updated as changes occur. In addition the Circular states that "manual procedures are generally NOT [emphasis in original] a viable back-up option."

Cause:

Service Center officials said that update of the risk analysis and continuity of operations plan had low priorities. In addition, Service Center officials stated that the FFS application was not included in the Plan as a result of Service Center clients agreeing that FFS services could be delayed for 30 days because processing **could be** performed manually. However, we found no documentation of such agreements.

Effect:

If the Continuity of Operations Plan is incorrect (such as by not including all sensitive systems) or is outdated, personnel required to perform the disaster recovery procedures may not be able to recover critical systems in the event of a disaster or system failure.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Perform a risk analysis of the Service Center's computer center and its applications.

Response

Complied. A risk analysis of the computer center was completed in November 1996. The security plan calls for periodic reviews of security controls for major systems in accordance with the requirements of OMB Circular A-130.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

2. Update the existing Continuity of Operations Plan for the mainframe, sensitive applications, and telecommunications links so that the current operating environment is documented.

Response

Concur. The Continuity of Operations Plan will be updated for the mainframe, sensitive applications and telecommunication links by September 30, 1997. The responsible official is the Chief, ADP Services Division. It should be noted that we believe this condition should have been more appropriately stated as a currency of documentation issue. The ASC has addressed recovery of the Federal Financial System and telecommunications although not formally documented. This will now be documented as part of the update of the Continuity of Operations Plan.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

O. Comprehensive Business Recovery Plan

Condition: No comprehensive business recovery plan had been developed for the Service Center.

The only plan in existence at the Service Center was the Continuity of Operations Plan, which addressed only the recovery of the systems environment. The Plan did not address business and user operations that need to be in effect for the Service

Center to support its clients in the event of a disaster or system failure.

Criteria: Office of Management and Budget Circular A-130 requires agencies to establish

controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, generally accepted information systems standards recognize that a comprehensive business recovery plan is necessary to ensure the timely recovery of all business functions and of the systems environment, both of which are critical for day-to-day operations, and to minimize

down time.

Cause: The Service Center's emphasis was on the restoration of the mainframe environment

rather than on the recovery of business operations.

Effect: If a disaster or system failure occurs, the Service Center may not be able to recover

all business functions and systems necessary for the continued long-term operations

of the organization.

Recommendation

We recommend that the Director, Administrative Service Center, develop a comprehensive business recovery plan, which includes procedures for its business functions.

Response

Concur with intent. Although, we are not aware of any specific requirement for a "comprehensive business recovery plan," we are willing to evaluate major operations and business functions to ensure long-term sustainability. Completion of the evaluation is targeted for March 31, 1998. The responsible official is the Chief, Management Services Division.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required	
A.1, D.1, D.2, E.1, F.1, F.2, F.3, H.1, H.2, I.2, J.2, M.1, and N.1	Implemented.	No further action is required	
B.1, C.1, D.3, G.1, G.2, I.1, J.1, K.1, N.2, and O.1	Resolved: not implemented.	No further response to the Department of the Interior Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.	
L.l	Unresolved.	Reconsider the recommendation, and provide an action plan that includes target dates and titles of officials responsible for implementation.	

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

Within the Continental United States

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240 Our 24-hour Telephone HOTLINE 1-800-424-5081 or (202) 208-5300

TDD for hearing impaired (202) 208-2420 or 1-800-354-0996

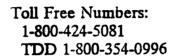
Outside the Continental United States

Caribbean Region

U.S. Department of the Interior Office of Inspector General Eastern Division - Investigations 1550 Wilson Boulevard Suite 410 Arlington, Virginia 22209 (703) 235-9221

North Pacific Region

U.S. Department of the Interior Office of Inspector General North Pacific Region 238 Archbishop F.C. Flores Street Suite 807, PDN Building Agana, Guam 96910 (700) 550-7428 or COMM 9-011-671-472-7279



FTS/Commercial Numbers: (202) 208-5300 TDD (202) 208-2420

1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240





U.S. Department of the Interior Office of Inspector General

EVALUATION REPORT

YEAR 2000 READINESS OF AUTOMATED INFORMATION SYSTEMS AT THE BUREAU OF INDIAN AFFAIRS

> REPORT NO. 98-I-479 JUNE 1998



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL. Washington, D.C. 20240

JUN - 5 1998

EVALUATION REPORT

Memorandum

Assistant Secretary for Indian Affairs To:

The Special Trustee for American Indians

From:

Robert J. Williams Pobut J. Wielesian Acting Inspector General

Subject: Evaluation Report on the Year 2000 Readiness of Automated Information

Systems at the Bureau of Indian Affairs (No. 98-1-479)

INTRODUCTION

This report presents the results of our evaluation of the year 2000 (Y2K) readiness of automated information systems at the Bureau of Indian Affairs. The objective of our review was to determine whether the Bureau (1) inventoried its automated information systems and identified those systems that were mission critical and were not Y2K compliant. (2) developed auditable cost estimates for renovating systems to be Y2K compliant, (3) identified by name an individual responsible for ensuring that the Bureau is Y2K compliant, (4) ensured that responsible individuals' personnel performance evaluation plans included critical elements related to identifying and remedying Y2K problems, (5) developed a credible plan that included milestones and a critical path to ensure that the Bureau is Y2K compliant, and (6) developed a contingency plan that would address the failure of any part of the systems not being Y2K ready. This review was conducted at the request of the Department of the Interior's Chief Information Officer to assist the Information Officer in monitoring the progress of Departmental agencies in ensuring Y2K readiness, implementing Y2K compliant systems, and validating the accuracy of the information reported by the bureaus and Departmental offices to the Chief Information Officer.

BACKGROUND

The "Y2K problem" is the term used to describe the potential failure of information technology systems, applications, and hardware related to the change to the year 2000. Many computers that use two digits to keep track of the date will, on January 1, 2000, recognize "double zero" not as 2000 but as 1900. This could cause computers to stop running or to start generating erroneous data. The problem has been recognized as nationally

significant by the President in Executive Order No. 13073, issued in February 1998. The Secretary of the Interior, in a December 1997 memorandum, stated that the Y2K problem was critical to the Department's meeting its mission and that resolution of the problem was one of his highest priorities. Further, Office of Management and Budget Memorandum 98-02, "Progress Reports on Fixing Year 2000 Difficulties," issued on January 20, 1998, requires all Federal executive branch agencies, to ensure that Federal Government systems do not fail in the year 2000, to have all systems, applications, and hardware renovated by September 1998; validated by January 1999; and implemented (that is, "fixes to all systems-both mission critical and nonmission critical") by March 31, 1999, to ensure that Federal Government systems do not fail in the year 2000. The Office of Management and Budget states in Memorandum 98-02 that it is to provide "information to the Congress and the public as part of its [Office of Management and Budget's] quarterly summary reports on agency progress . . . [and] to report on the status of agency validation and contingency planning efforts and on progress in fixing . . . equipment that is date sensitive."

The Department has a multitiered approach to managing the Y2K problem that includes a top tier comprising the Secretary of the Interior; the Information Technology Steering Committee, which comprises the Chief of Staff and Assistant Secretaries; and the Chief Information Officer, who is responsible for the Department's Y2K issues. This tier, which represents senior-level Departmental managers, provides the Y2K project's overall direction and resources and ensures accurate reporting to external organizations such as the Office of Management and Budget and the Congress. A Departmentwide Y2K project team, which reports to the Chief Information Officer and comprises representatives from each agency and the Office of the Secretary, is tasked with developing the Department's Year 2000 Management Plan, refining inventory data on the Department's mission-critical and information technology portfolio systems, and monitoring and reporting the progress of each conversion. In addition, a Y2K Embedded Microchip² Coordinators Team has been established to inventory and monitor embedded microchip technology Y2K problems. The team is led by the Office of Managing Risk and Public Safety and comprises representatives of the eight Departmental bureaus, the Denver Administrative Service Center, and various Departmental offices. The Department has developed the "Department of the Interior Year 2000 Management Plan," which focuses on resolution of the Y2K problem and provides an overall strategy for managing Departmental mission-critical systems and infrastructure.

The Department's February 1998 "Year 2000 Management Plan," which was submitted to the Office of Management and Budget, reported that the Department had 95 mission-critical systems. Of the 95 mission-critical systems reported by the Department to the Office of Management and Budget, the Bureau of Indian Affairs and the Office of the Special Trustee

¹The portfolio systems is an inventory listing of 13 cross-cutting or sensitive systems that are receiving attention at the Secretarial level.

²Embedded microchips are "integrated circuits (miniature circuit boards)" that "control electrical devices" which include "elevators; heating, ventilation, and air conditioning (HVAC) systems; water and gas flow controllers; aircraft navigational systems; and . . . medical equipment" and office devices such as telephones, facsimile machines, pagers, and cellular telephones. (Department of the Interior's Office of Managing Risk and Public Safety "Year 2000 Embedded Microchip Hazards" [Website]).

for American Indians had 15 systems (see Appendix 1), of which 4 are included in the Department's information technology portfolio.³ To address the Y2K problems, the Bureau and the Office of the Special Trustee established a project management team comprising senior executives and a task group. The senior executives are the Acting Director, Office of Management and Administration, Bureau of Indian Affairs, and the Deputy Director for Operations, Office of the Special Trustee. The task group comprises a manager and a coordinator from the Office of Information Resources Management and nine members from the Bureau's Operations Service Center (3) and other Program offices (5) and the Office of the Special Trustee's Office of Trust Funds Management.

SCOPE OF EVALUATION

To accomplish our objective, we reviewed the documentation available that supported the Bureau of Indian Affairs information submitted to the Department's Chief Information Officer through February 1998. We performed our review at the Bureau's Operations Service and Facilities Management and Construction Centers and the Office of the Special Trustee for American Indians Office of Trust Funds Management, all of which are located in Albuquerque, New Mexico. We interviewed personnel responsible for project coordination to identify the Bureau's Y2K plans and progress. We also interviewed personnel involved in various aspects of the Y2K project, including coordination, compliance identification, software remediation, and project management.

The evaluation was conducted in accordance with the "Quality Standards for Inspections," issued by the President's Council on Integrity and Efficiency and, accordingly, included such tests and inspection procedures considered necessary to accomplish the objective. Our conclusions on the status of the progress made by the Bureau in addressing and remediating Y2K problems were based on reviews of documentation maintained by the Operations Service Center and discussions with the Y2K coordinator and the Y2K task group members who performed remediation or replacement of noncompliant applications or hardware. As specifically agreed to in our discussions with the Department's Chief Information Officer, we did not validate or certify that the Bureau's systems were Y2K compliant.

³The four Bureau of Indian Affairs and Office of the Special Trustee for American Indians applications or systems contained in the Department's information technology portfolio are the Individual Indian Monies (IIM); Land Records Information System (LRIS); Omni Trust ES; and Facilities, Construction, Operations, and Maintenance (FACCOM) system.

⁴The Bureau of Indian Affairs is responsible for remediating the Y2K problem for existing systems, such as the Individual Indian Monies system of the Office of Trust Funds Management, Office of the Special Trustee for American Indians.

RESULTS OF EVALUATION

Although the Bureau's Y2K project management had begun to identify systems and had developed a master plan for remedying Y2K problems, it had not completed any of the six objectives that the Chief Information Officer had requested us to evaluate. The specific actions taken by the Bureau related to each objective are discussed in the paragraphs that follow. As a result of not completing the objectives, we believe that there is an increased risk that the Bureau may not meet the Office of Management and Budget's target date of March 1999 for having compliant Y2K systems implemented. The Bureau has recently awarded contracts to assist in its assessment, renovation, and implementation of compliant systems; therefore, we have not made any recommendations. However, the Bureau should ensure that sufficient resources are made available to meet its milestone dates.

Automated Information Systems Inventory

All of the Bureau's mission- and nonmission-critical automated information systems may not have been included in its inventory. According to the Department's milestone dates, agencies were required to have mission-critical systems inventoried and systems that were not Y2K compliant identified by June 1997. Although national systems that were deemed mission critical⁵ by the Bureau had been identified and noncompliance had been determined, 8 of the 12 Bureau area offices and 10 of 15 Bureau program and division offices had not responded to inventory requests made by the Bureau's Director, Office of Management and Administration, dated January, July, and September 1997. Therefore, the Bureau had little assurance that all mission- and nonmission-critical systems had been identified and reported to the Department's Chief Information Officer.

Auditable Cost Estimates

The documentation used to support the Bureau's cost estimates for correcting the Y2K problem in each of the Bureau's 15 mission-critical systems was not maintained. To accurately report the costs associated with correcting the Y2K problem, Office of Management and Budget guidelines state that costs to rectify noncompliant Y2K systems should be specifically related to Y2K efforts, such as repairing the lines of source code⁶ or replacing the systems. If a noncompliant system is to be replaced for reasons not specifically attributable to Y2K, the cost of replacement should not be reported as a cost to correct the Y2K problem. However, any contract costs that are associated with the Bureau's efforts in assessing, renovating, and implementing Y2K-ready systems should be included in the Bureau's cost estimates.

⁵These systems were deemed mission critical based on the systems' effect on accounting for and distributing funds to organizations, tribes, and individual Indians.

⁶Lines of source code are statements and instructions used by the computer to execute the tasks of computer programs. (Computer Desktop Encyclopedia, Version 9.4, 4th quarter, 1996)

Although the Bureau's cost estimates were not auditable, we attempted to determine whether the methodology used by the Y2K task group to develop cost estimates was reasonable based on a "re-creation" of cost estimates for 2 of the 15 systems. The original methodology used by the Bureau was based on an estimate of the percentage of date-sensitive lines of source code to the total number of lines of source code multiplied by the Gartner Group's estimated cost of \$1.70 per line of source code to be corrected. We determined that the methodology used to develop the costs was reasonable; however, the estimates had not been updated to reflect more recent information that may affect the estimates. For example, applications that run on the UNISYS platform were being "cleaned up" by deleting unnecessary lines of source code, including the Oil and Gas module that had its total lines of source code reduced from 43,989 to 41,250. The methodology used by the Bureau may require that the estimated lines of source code requiring remediation and the associated cost estimate be reduced. Also, the cost to correct the Facilities, Construction, Operations, and Maintenance (FACCOM) system, which is run on the IBM mainframe platform, for Y2K compliance will not be accomplished through the code remediation effort, as originally anticipated by the Bureau. Instead, the FACCOM system is scheduled to be replaced by March 1999. The replacement system is necessary to allow the system to operate with current mainframe or client/server operating systems, not for reasons directly related to correcting Y2K problems. Therefore, the estimated cost of \$254,000 reported to correct the Y2K problem for the FACCOM system was overstated.

In addition, the cost of \$4.8 million to remediate the Y2K problem in the Individual Indian Monies (IIM) system as reported to the Department was incorrect. The \$4.8 million was the estimated cost for the first year of development and implementation of the IIM replacement system. The IIM is being replaced for a number of reasons, such as to meet the requirements mandated by the American Indian Trust Fund Management Reform Act of 1994, not just to correct the Y2K problem; therefore, the \$4.8 million reported to remediate the Y2K problem was overstated. However, because the IIM replacement system is not planned to be implemented until after the year 2000, costs to repair the existing system should be estimated and reported to the Department.

Designation of Responsible Individuals

The Departmental Chief Information Officer requested that we determine whether responsible officials had been specifically named. As of March 18, 1998, the Assistant Secretary for Indian Affairs had designated, by title, the Y2K executive; by office, the Y2K coordinating office; and by name, the individuals who made up the Y2K task group. In addition, a representative from the Office of the Special Trustee was included as part of the

⁷A computer services company that provides independent advice to business professionals making information technology decisions.

⁸The task group estimated that about 10 percent of its total lines of source code were date sensitive. For example, if a system had 425,000 lines of source code, 42,500 lines of source code would be date sensitive and thus would require repair. The 42,500 was then multiplied by the Gartner Group's cost estimate of \$1.70 to repair a line of source code, which would result in an estimated cost of \$72,250.

Bureau's Y2K task group. We believe that designating the Y2K executive by title and the Y2K coordinating office by office rather than by name and title of individuals did not meet the intent of the Chief Information Officer's request to have responsible individuals named.

Annual Personnel Performance Evaluation Plans

The Secretary of the Interior's December 1997 memorandum and the Assistant Secretary for Indian Affairs February 1998 memorandum required that "a critical performance element for identifying and remedying the Y2K" problem be included as part of each responsible official's annual performance plan. Responsible officials are defined in the memorandum as agency directors, agency Y2K executives, agency information resources management coordinators, safety officials, and all others as determined by the Y2K executive. In addition, the Assistant Secretary required that the elements be included in the annual personnel performance plans by February 27, 1998. However, as of March 18, 1998, we found that except for one member of the Y2K task group, the elements were not included in the annual personnel performance plans of the Bureau's and the Office of the Special Trustee's Y2K executives and the individual members of the Y2K task group, which included the Director, Information Resources Management.

Plan for Milestones

We found no documentation to support the milestones established by the Bureau. The 15 systems included in the Bureau's inventory were being evaluated and remediation was planned for Y2K compliance. However, the milestone dates established in the Bureau's Y2K master plan for analyzing existing code had slipped by approximately 2 months. According to a member of the Y2K task group, these dates were not met because the software tool planned for use in identifying and assisting in remediating lines of source code was originally estimated to be available in January 1998; however, as of March 18, 1998, the tool had not been purchased. Therefore, the current Y2K master plan may not reflect achievable milestone dates. However, Bureau officials indicated at the exit conference and in the Bureau's written response that they believed the acquisition of the "Millennium Solution" tool has brought the Bureau back on schedule.

Contingency Plans

We found that a formal contingency plan had been developed for only 1 of the 15 mission-critical systems. Since the milestone dates established by the Bureau have slipped by approximately 2 months, there may be a need for formalizing contingency plans for the remaining 14 systems. If additional mission-critical systems are subsequently identified (see section "Automated Information Systems Inventory" in this report), contingency plans for these systems may also need to be developed. However, the Y2K task group member responsible for the Bureau's application software and national systems stated that once the software tool was acquired, the milestone dates established in the master plan for the 15 systems could be met through personnel efforts such as increasing the number of shifts worked and the number of contractor staff.

Other Issues

The Department of the Interior and the Office of Management and Budget required that an inventory of all data exchanges with outside parties be completed by February 1, 1998, and that coordination with these parties to determine a transition plan occur by March 1, 1998. The Assistant Secretary for Indian Affairs had established a March 30, 1998, target date for the Y2K task group to contact the tribes and tribal organizations to ensure that systems which interface with Bureau systems are Y2K compliant. However, we found that the letter requesting information from the Bureau's data exchange partners to accomplish the coordination effort had not been issued as of March 18, 1998.

The Bureau has reported to the Departmental Chief Information Officer that it has four systems which are compliant except for independent verification and validation. However, the Bureau has not conducted regression testing, integrated testing, or Y2K testing on these systems. Instead, the Bureau's Y2K project management has relied on the recent design and implementation of these systems.

On May 12, 1998, we held an exit conference to discuss a preliminary draft of the report with Y2K officials from the Bureau and the Office of the Special Trustee and with the Department's Deputy Chief Information Officer. Office of the Special Trustee officials generally agreed with our findings but provided no written response to the report. Bureau officials also generally agreed with our findings and provided additional information in a May 15, 1998, response (see Appendix 2). Based on the discussions and the response, we made changes to the report as appropriate; however, we did not revise our report to reflect changes or improvements made by the Bureau since March 18, 1998. In its response, the Bureau stated that contracts had been awarded and corrective actions were being taken to ensure that its automated information systems will be Y2K compliant.

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, the monetary impact of audit findings, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of personnel at the Bureau of Indian Affairs and the Office of the Special Trustee for American Indians in the conduct of our audit.

⁹In software development, "regression testing" is defined as "testing a program that has been modified in order to ensure that additional bugs have not been introduced." (<u>Computer Desktop Encyclopedia</u>, Version 9.4, 4th quarter, 1996.)

¹⁰"Integrated" is defined as "a collection of distinct elements or components that have been built into one unit." (Computer Desktop Encyclopedia, Version 9.4, 4th Quarter, 1996.)

BUREAU OF INDIAN AFFAIRS MISSION-CRITICAL SYSTEMS INVENTORY'

System Name or Acronym	Description	Estimated Cost for
System Name of Actoriyin	Description	Compliance
Social Services	A system that processes general assistance payments to individual Indians.	\$72,250
Individual Indian Monies (IIM)	Tracks funds due individual Indians and tribes from leasing, permits, and other uses of Indian lands. (Interfaces with IRMS.)	\$4,800,000
Land Records Information System (LRIS)	A land title system showing and tracking Indian ownership, including all rights conveyed or changed over time. Provides official reports for title status and probate inventory.	\$68,000
Omni Trust ES	A system for tracking funds applied to Indian trust accounts and allotments to individual Indians. Records investing and payout information. (Interfaces with IRMS.)	0
Facilities, Construction, Operations, and Maintenance (FACCOM)	Maintains facilities inventory data, prioritizes deferred maintenance deficiencies, monitors progress of constructions projects, and calculates operations and maintenance funding for all property owned or operated by the Bureau of Indian Affairs.	\$254,000
National Indian Irrigation Management System (NIIMS)	Tracks and bills assessments for costs of operations and maintenance of Indian irrigation projects to be reimbursed to the Government.	\$42,500

^{*}Information for system name or acronym and for description is from the Bureau of Indian Affairs, and information for estimated costs is from the February 1998 "Department of the Interior Year 2000 Management Plan."

System Name or Acronym	Description	Estimated Cost for Compliance
Lease/Range - Subsystem of the Integrated Records Management System (IRMS)	A system for managing payouts for leases on Indian lands, based on interests in contracts on Indian lands.	\$43,000
Owner - Subsystem of the Integrated Records Management System (IRMS)	A system that tracks ownership of Indian tribal and trust lands.	\$35,000
People - Subsystem of the Integrated Records Management System (IRMS)	A census and demographic database on individuals who are enrolled members of tribes or who have interests in Indian trust assets.	\$34,700
Royalty Distribution and Reporting System (RDRS)	A tracking system for mineral and surface land ownership for oil and mineral leases.	\$9,200
Lease Distribution	A payout system for leases on Indian trust lands	\$1,700
Loan Management Accounting System (LOMAS)	A loan management and accounting system for economic development programs.	0
Osage Annuity System	A system to pay out monies to members of the Osage Tribe who are decedents of the original Head Right owners.	0
Tribal Allocation Priority System (TAPS)	A system that is used to develop budget estimates based on tribal priorities.	\$5,000
Land Title Mapping System (GIS)	A geographical information system (GIS) that has been tailored to support the use and application of spatial data technologies throughout the Bureau of Indian Affairs. Reports boundary and ownership in a land status map.	0
	Total	<u>\$5,365,350</u>



United States Department of the Interior

BUREAU OF INDIAN AFFAIRS

INFORMATION RESOURCES MANAGEMENT OPERATIONS SERVICE CENTER 500 GOLD AVENUE, S.W.

P.O. BOX 888

ALBUQUERQUE, NEW MEXICO 87103

Memorandum

May 15, 1998

To:

Diane Sandy, Office of Inspector General

Department of the Interior

Linda Richardson, Office of Audit & Evaluations

Bureau of Indian Affairs

From:

Nancy Jemison, Year 2000 Executive

Bureau of Indian Affairs

Subject:

Year 2000 Review

This is a follow up the telephone exit conference held on Tuesday May 12, 1998.

Attached, you will find the Bureau of Indian Affairs (BIA) response to the Year 2000 audit review. Also attached, you will find a working draft, of the BIA Year 2000 Master Plan.

During the telephone exit conference reference was make about publishing this information to the IG Web site. The BIA's Y2K Master Plan is a working draft, for this reason we do not want this document published on any Web site, at this point in time.

RESPONSE TO DOI INSPECTOR GENERAL'S SURVEY REPORT YEAR 2000 REVIEW BY THE BUREAU OF INDIAN AFFAIRS

15 MAY 1998

Automated Information Systems Inventory

All of the Bureau's mission and nonmission-critical automated information systems may not have been included in its inventory. According to the Department's milestone dates,

agencies were required to have mission-critical systems inventoried and systems that were not Y2K compliant identified by June 1997. Although national systems that were deemed mission critical by the Bureau had been identified and noncompliance had been determined, 8 of the 12 Bureau area offices and 10 of 15 Bureau program and division offices had not responded to inventory requests made by the Bureau's Director, Office of Management and Administration, in January, July, and September 1997. Therefore, the Bureau had little assurance that all mission and nonmission-critical systems had been identified and reported to the Department's Chief Information Officer.

BIA Response:

The BIA has placed our highest priority on the inventory of National Systems, which are mission critical. BIA's OIRM OSC is responsible for maintaining all the National Applications, most of which are housed on the Unisys platform in ALBQ or on the IBM in Reston at USGS. BIA expected a small response to the inventory request of these national systems from area, agency or school offices.

We recognize that there may be local safety and/or program essential systems in local facilities. In order to gain cooperation from areas, agencies and schools, the BIA Y2K team has visited the following areas as of May 15: Aberdeen, Billings, Navajo, Portland, Phoenix, and Sacramento. The Y2K Team will visit the remaining Areas within the next 30 days. The result of our visits is a much higher participation from local offices. As of May 15, 70% of POC information for embedded systems and telecommunications equipment have been received from areas and agencies. These data are being entered into an Inventory Database. With the help of Mitretek, we are in the process of sending a second data call (See Attachment 1), via the use of electronic forms, to collect inventory data of less critical components such as personal computers, office automation software, local databases, etc. Mitretek is also helping the BIA develop a Year 2000 web site (See Attachment 2 for sample screens of the IHS Web site) to facilitate information dissemination and local systems/software/hardware inventory and assessment. Area, agency and school Y2K POCs who have Internet access will be able to enter and update inventory data for local facilities, check compliance status of hardware/software against known baseline compliance data and/or using procedures, and generate compliance status reports online. Tribes are also encouraged to take advantage of this facility to support their Y2K compliance needs.

Auditable Cost Estimates

These systems were deemed mission critical based on the system's effect on accounting for and distributing funds to organizations, tribes, and individual Indians.

The documentation used to support the Bureau's cost estimates for correcting the Y2K problem in each of the Bureau's 15 mission-critical systems was not maintained. To accurately report the costs associated with correcting the Y2K problem, Office of Management and Budget guidelines state that costs to rectify noncompliant Y2K systems should be specifically related to Y2K efforts, such as repairing the lines of source code' or replacing the systems. If a noncompliant system is to be replaced for reasons not specifically attributable to Y2K, the cost of replacement should not be reported as a cost to correct the Y2K problem. However, any contract costs that are associated with the Bureau's efforts in assessing, renovating, and implementing Y2K-ready systems should be included in the Bureau's cost estimates. Although the Bureau's cost estimates were not auditable, we attempted to determine whether the methodology used by the Y2K task group to develop cost estimates was reasonable based on a 're-creation' of cost estimates for 2 of the 15 systems. The original methodology used by the Bureau was based on an estimate of the percentage of date-sensitive lines of source code to the total number of lines of source code multiplied by the Gartner Group's' estimated cost of \$1.70 per line of source code to be corrected. We determined that the methodology used to develop the costs was reasonable; however, the estimates had not been updated to reflect more recent information that may affect the estimates. For example, applications that run on the UNISYS platform were being cleaned up by deleting unnecessary lines of source code, including the Oil and Gas module that had its total lines of source code reduced from 48,989 to 41,250. The methodology used by the Bureau would require that the estimated lines of source code requiring remediation and the associated cost estimate be reduced. Also, the cost to correct the Facilities, Construction, Operations, and Maintenance (FACCOM) system, which is run on the IBM mainframe platform, for Y2K compliance will not be accomplished through the code remediation effort, as originally anticipated by the Bureau. Instead, the FACCOM system is being replaced by March 1999 because the source code cannot be remediated so that the system can operate with current mainframe or client/server operating systems, not for reasons directly related to correcting Y2K problems. Therefore, the estimated cost of \$254,000 reported to correct the Y2K

Lines of source code are statements and instructions used by the computer to execute the tasks of computer programs. (Computer Desktop Encyclopedia, Version 9.4, 4th quarter, 1996)

^{&#}x27;A computer services company that provides independent advice to business professionals making information technology decisions.

^{&#}x27;The task group estimated that about 10 percent of its total lines of source code were date sensitive. For example, if a system had 425,000 lines of source code, 42,500 lines of source code would be date sensitive and thus would require repair. The 42,500 was then multiplied by the Gartner Group's cost estimate of \$1.70 to repair a line of source code, which would result in an estimated cost of \$72,250.

problem for the FACCOM system was overstated.

In addition, the cost of \$4.8 million to remediate the Y2K problem in the Individual Indian Monies (IIM) system as reported to the Department was incorrect. The \$4.8 million was the estimated cost for the first year of development and implementation of the IIM replacement system. The IIM is being replaced for a number of reasons, such as to meet the requirements mandated by the American Indian Trust Fund Management Reform Act of 1994, not just to correct the Y2K problem; therefore, the \$4.8 million reported to remediate the Y2K problem was overstated. However, because the IIM replacement system is not planned to be implemented until after the year 2000, costs to repair the existing system should be estimated and reported to the Department.

BIA Response:

The BIA is in the process of setting up a project file, included in the file will be all support documentation for cost estimates. With Mitretek's help, the BIA is developing a Year 2000 Master Plan (See Attachment 3 for a working draft of the BIA Y2K Master Plan). The Plan more accurately accounts for Year 2000 compliance expenses.

The BIA Y2K coordinator had submitted an estimate of \$62K for the Year 2000 remediation of the IIM sub-system to the DOI Y2K coordinator more than one year ago. DOI Office of the Special Trustee had submitted Y2K information to the same DOI Y2K coordinator. A decision inside DOI led to the decision to include \$4.8 million as the Year 2000 cost for IIM replacement, instead of \$62K supplied by BIA.

Designation of Responsible Individuals

The Assistant Secretary for Indian Affairs designated, by title, the Y2K executive; by office, the Y2K coordinating office; and by name, the individuals who made up the Y2K task group. In addition, a representative from the Office of the Special Trustee was included as part of the Bureau's Y2K task group. The Departmental Chief Information Officer requested that we determine whether responsible officials had been specifically named. We believe that designating responsible individuals by title rather than by name and title did not meet the intent of the Chief Information Officer's request to have responsible individuals named.

BIA Response:

The BIA has a Year 2000 project team which was formed in February 1998. The Director of Management and Administration is the BIA Year 2000 Executive who is responsible for ensuring overall Year 2000 compliance within the BIA, while the Office of

Information Resources Management is serving as the Year 2000 coordinating office within the BIA. The Director of Facilities Management is serving as the BIA's Embedded Technology Executive. In addition, the following staff is serving on the BIA's Year 2000 Task Group:

Nancy Jemison Year 2000 Executive George Gover Year 2000 Manager

Bill Collier, Jr. Year 2000 Embedded System Executive

Ed Socks Year 2000 Coordinator

Mona Infield Year 2000 Application Software & National Systems

Ron Shepherd Year 2000 WAN/LAN

Don Mayer Year 2000 Mainframe Hardware & Software
Dr. Ken Ross Year 2000 Office of Indian Education Programs

Al Lindfors Year 2000 Embedded Chip
Byron Carr Year 2000 Telephone/Voice/Data

Bob McKenna Year 2000 Office of Trust Funds Management

Craig Jones Year 2000 Law Enforcement
Bill Bonner Year 2000 GIS Systems

The BIA's Year 2000 Task Group is expected to grow as Year 2000 efforts progress throughout the BIA's Area Offices, Agencies, program offices and schools. These local offices have begun to form local Year 2000 task groups dedicated to the Year 2000 compliance effort. To assist in project management and other Year 2000 activities, the BIA has selected Mitretek, an independent contractor, to assist the Year 2000 Task Group and report its progress to the BIA's Year 2000 Executive.

Annual Personnel Performance Evaluation Plans

The Secretary of the Interior's December 1997 memorandum and the Assistant Secretary for Indian Affairs February 1998 memorandum required that "a critical performance element for identifying and remedying the Y2K" problem be included as part of each responsible official's annual performance plan. Responsible officials are defined as agency directors, agency Y2K executives, agency information resources management coordinators, safety officials, and all others as determined by the Y2K executive. In addition, the Assistant Secretary required that the elements be included in the annual personnel performance plans by February 27, 1998. However, as of March 18, 1998, we found that except for one member of the Y2K task group, the elements were not included in the annual personnel performance plans of the Bureau's and the Office of the Special Trustee's Y2K executives and the individual members of the Y2K task group, which included the Director, Information Resources Management.

BIA Response:

The BIA Y2K Executive had sent out a memo to all areas, agencies and schools for this purpose 10 days before IG's visit. Due to the wide geographical distribution of the BIA's offices, it takes about 2 weeks for the information to be communicated to the lower levels of the field offices. This could explain why most of the Y2K project staffers didn't have it included in their annual performance plan at the time of IG's audit. We believe this has become standard practice today. Additionally, the BIA will have a critical performance element for identifying and remedying the Y2K added for all field staff who are designated as Y2K Point of Contacts(POC).

Plan for Milestones

We found no documentation to support that the milestones established by the Bureau were achievable. Furthermore, even though the 15 systems included in the Bureau's inventory were being evaluated and remediation was planned for Y2K compliance, the milestone dates established in the Bureau's Y2K master plan had slipped by approximately 2 months. According to a member of the Y2K task group, these dates were not met because the software tool planned for use in identifying and assisting in remediating lines of source code was originally estimated to be available in January 1998; however, as of March 18, 1998, the tool had not been purchased. Therefore, the current Y2K master plan may not reflect achievable milestone dates.

BIA Response:

DII has demonstrated to BIA its Millennium Solution tool. BIA has tested the tool and has been using the tool for assessment and code remediation for the last month. The Master Plan had not been slipped by 2 months.

Milestones and resource requirements are well documented in the attached Year 2000 Master Plan.

Contingency Plans

We found that a formal contingency plan had been developed for only 1 of the 15 mission-critical systems. Since the milestone dates established by the Bureau have slipped by approximately 2 months, there may be a need for formalizing contingency plans for the remaining 14 systems. If additional mission-critical systems are subsequently identified (see Section 'Automated Information Systems Inventory' in this report), contingency plans for these systems may also need to be developed. However, the Y2K task group member responsible for the Bureau's application software and national systems stated that once the

software tool was acquired, the milestone dates established in the master plan for the 15 systems could be met through personnel efforts such as increasing the number of shifts worked and increasing the number of contractor staff.

BLA Response:

The BIA will be developing detailed contingency plans as part of the BIA Y2K Master Plan.

Other Issues

The deadline established by the Department of the Interior and the Office of Management and Budget required that an inventory of all data exchanges with outside parties be completed by February 1, 1998, and that coordination with these parties to determine a transition plan occur by March 1, 1998. The Assistant Secretary for Indian Affairs had established a March 30, 1998, target date for the Y2K task group to contact the tribes and tribal organizations to ensure that systems which interface with Bureau systems are Y2K compliant. However, we found that the letter requesting information from the Bureau's data exchange partners to accomplish the coordination effort had not been issued as of March 18, 1998.

BIA Response:

The BIA has sent a letter on 31 March 1998 to all known Data Exchange partners, some of which happened to be Tribes. No letters were sent to those Tribes that do not have data exchange with the BIA's systems. As a way of providing Y2K support to the Tribes, we invite Tribes to BIA local Year 2000 information meetings and we plan to share our Year 2000 knowledge base with the Tribes through the use of our Year 2000 web in the near future.

The Bureau has reported to the Departmental Chief Information Officer that it has four systems that are compliant except for independent verification and validation. However, the Bureau has not conducted regression testing, integrated testing, or Y2K testing on

^{&#}x27;In software development, "regression testing" is defined as "testing a program that has been modified in order to ensure that additional bugs have not been introduced." (Computer Desktop Encyclopedia, Version 9.4, 4th quarter, 1996.)

[&]quot;Integrated" is defined as "a collection of distinct elements or components that have been built into one unit." (Computer Desktop Encyclopedia, Version 9.4, 4th Quarter, 1996.)

these systems. Instead, the Bureau's Y2K project management has relied on the recent design and implementation of these systems.

BIA Response:

The BIA has contracted for Y2K testing support, Anteon has been selected to develop a test plan that will address tests mentioned above. A schedule for conducting these tests is included in the attached Year 2000 Master Plan.

If you have any questions on these materials, please refer questions to Ed Socks. Mr. Socks served as the audit coordinator for this review, office number 505-248-7156, email address: ed_socks@mail.bia.gov

[NOTE: YEAR 2000 MASTER PLAN NOT INCLUDED BY OFFICE OF INSPECTOR GENERAL.]

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

Within the Continental United States

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240 Our 24-hour Telephone HOTLINE 1-800-424-5081 or (202) 208-5300

TDD for hearing impaired (202) 208-2420 or 1-800-354-0996

Outside the Continental United States

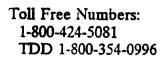
Caribbean Region

U.S. Department of the Interior Office of Inspector General Eastern Division - Investigations 1550 Wilson Boulevard Suite 410 Arlington, Virginia 22209

(703) 235-9221

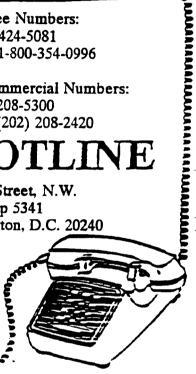
North Pacific Region

U.S. Department of the Interior Office of Inspector General North Pacific Region 238 Archbishop F.C. Flores Street Suite 807, PDN Building Agana, Guam 96910 (700) 550-7428 or COMM 9-011-671-472-7279



FTS/Commercial Numbers: (202) 208-5300 TDD (202) 208-2420

1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240





U.S. Department of the Interior Office of Inspector General

AUDIT REPORT

FOLLOWUP OF GENERAL CONTROLS
OVER AUTOMATED INFORMATION SYSTEMS,
OPERATIONS SERVICE CENTER,
BUREAU OF INDIAN AFFAIRS

REPORT NO. 98-I-483 JUNE 1998



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

JUN 1 0 1998

AUDIT REPORT

Memorandum

To:

Assistant Secretary for Indian Affairs

From:

Robert J. Williams Kobert & Williams

Acting Inspector General

Subject: Audit Report on Follow-up of General Controls Over Automated Information

Systems, Operations Service Center, Bureau of Indian Affairs (No. 98-I-483)

INTRODUCTION

This report presents the results of our followup audit of recommendations contained in our April 1997 audit report titled "General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs" (No. 97-I-771). The objective of our followup audit was to determine whether the Bureau of Indian Affairs had satisfactorily implemented the recommendations made in our prior audit report and whether any new recommendations were warranted. This audit supports the annual financial statements audits of the Bureau and the Office of the Special Trustee for American Indians by evaluating the reliability of the general controls over computer-generated data that support the financial statements.

BACKGROUND

The Operations Service Center is organizationally under the Bureau's Office of Information Resources Management and is located in Albuquerque, New Mexico. The Center operated an IBM and a Unisys mainframe computer and provided computer services such as telecommunications; software development, operations, and maintenance; systems recovery; and user support and is responsible for the Bureau's automated information system security. The IBM computer was used to run Bureau applications such as the Land Records Information System and the National Irrigation Information Management System. The Unisys computer was used to run Office of the Special Trustee for American Indians applications such as the Individual Indian Monies application and Bureau applications that supported the Indian trust fund accounts.

In response to our prior audit, the Bureau informed us that the IBM and Unisys mainframe computer operations and data processing functions were being transferred to a host computer owned by the U.S. Geological Survey, located in Reston, Virginia. The operating and data processing functions provided by the Geological Survey were to allocate space on the host computer for the Bureau to operate and run its IBM operating system, applications, and security software; to provide for physical security over the host computer; to back up and recover data and files; and to provide off-site storage of backed up data and files.

SCOPE OF AUDIT

The scope of our **followup** audit included an evaluation of the actions taken by Bureau management to implement the 13 recommendations made in our April 1997 audit report. In addition, we reviewed the Bureau's progress in moving the Center's mainframe data processing functions to the Geological Survey's host computer in **Reston** because of the impact that moving the data processing functions will have on Bureau management's ability to implement the recommendations.

This review was conducted in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances. We reviewed internal controls only to the extent that they related to corrective actions taken by Bureau management on the recommendations contained in the April 1997 audit report.

RESULTS OF AUDIT

Our April 1997 audit report concluded that the general controls over the Bureau of Indian Affairs automated information systems at the Center were not effective. Specifically, an effective security program had not been implemented; controls over access, software development and changes, segregation of duties, and system software were inadequate; and a service continuity plan had not been developed and implemented. The general controls were not effective because Bureau management had not developed a formal, up-to-date, and comprehensive system security program or established formal policies, standards, and procedures for computer operations. Additionally, the Bureau's Information Technology (IT) Security Manager* function was not at the appropriate organizational level, and adequate funding and personnel were not provided to fully support the Center's mission. The audit concluded that the deficient general controls significantly increased the risk of unauthorized access; modifications to and disclosure of sensitive data maintained in the Center's mainframe computers; theft or destruction of hardware, software, and sensitive data; and loss of critical systems and functions in the event of a disaster. In addition, the deficient controls decreased the reliability of the data maintained on the Center's computers. Our April 1997 audit report contained 13 recommendations for improving the general controls over the Bureau's automated information systems at the Center.

^{&#}x27;This position was formerly known as the Bureau's Automated Information Systems Security Officer. The Departmental Manual (375 DM 19, "Information Technology Security") changed the title to "Bureau IT Security Manager."

Of the 13 recommendations made, we found that the Bureau had partially implemented 2 recommendations and had not implemented 10 recommendations and that 1 recommendation was no longer applicable because the Bureau changed its plans for the Unisys computer (see Appendix 1). Therefore, we concluded that the general control weaknesses and risks identified by our prior audit for fiscal year 1996 continued to exist during fiscal year 1997. We have made eight new recommendations to address the weaknesses we found during the followup audit.

In its response to the April 1997 audit report, the Bureau also stated that many of the weaknesses identified would be corrected with the movement of the Center's data processing functions to the Geological Survey's host computer. However, the Center will continue, at least for fiscal year 1998, to control, operate, and maintain its computer operating system and security software and to schedule production runs manually rather than use the Geological Survey's host computer operating, security, and automated job scheduling systems. Therefore, the control weaknesses increase the risk of loss of data integrity through fiscal year 1998. Accordingly, we believe that Bureau management should establish as a high priority the use of the Geological Survey's host computer systems to reduce the Bureau's risk of loss of data integrity. Additionally, management within the Bureau and the Office of the Special Trustee for American Indians did not move their applications that resided on the Center's Unisys mainframe to the Center's IBM mainframe, which would have then been moved to the Geological Survey's host computer, but instead planned to move their applications to the Unisys server. Thus the corrective actions outlined in the Bureau's response to the prior report that relied on the movement of all data processing functions from the Center to the Geological Survey were not completed.

In its response to the April 1997 audit report, the Bureau stated, "In conjunction with the transfer of mainframe data processing from the Bureau, some reorganization or redescription of positions within the Office of Information Resources Management will be necessary." The Bureau further stated that "completion of the reorganization is October 1, 1997 with an effective date of December 1, 1997." We found that Bureau management had not formally reorganized the Office of Information Resources Management but that Center management had informally reorganized the Center to prepare for providing services as a network management center. (A network management center provides enhanced customer support that uses advanced technologies for network connectivity and problem solving and developing and maintaining client/servers.*) Although the Center was being reorganized as a network management center, we did not find an approved strategic plan for such a center. As a result, corrective actions that were dependent on the reorganization of the Office of Information Resources Management were not completed.

²A "client/server" application functions on a client/server processing environment, which is a computerized architecture in which one or more "computers called servers manage shared resources and provide access to those shared resources as a service to their clients," which are personal computers. (David Vaskevitch, Client/Server Strategies. a Survival Guide for Corporate Reengineering, IDG Books Worldwide, Inc., San Mateo, California, 1993, page 96.)

Recommendation A. 1. The information technology security function be elevated organizationally to at least report directly to the Director, Office of Information Resources Management: is formally provided with authority to implement and enforce a Bureauwide system security program; and is provided staff to perform the reauired duties, such as providing commuter security awareness training; and performing periodic risk assessments.

Recommendation A.2. A system security program is developed and documented which includes the information reauired by the Commuter Security Act of 1987 and Office of Management and Budget Circular A- 130, Appendix III. and that Policies and procedures are implemented to keep the system security program current.

Regarding Recommendation A. 1,our prior audit found that because the Bureau's IT Security Manager function was within the Center, the security function did not have adequate independence or authority to implement and enforce a Bureauwide system security program. The security staff consisted only of the IT Security Manager and another staffperson. Most of the security staff's time was spent administering security at the Center and administering user access to the computer systems. Although users were provided written information about system security issues when access to computer systems and applications was approved, the Center did not have an employee computer security awareness training plan. Further, the security staff had not provided periodic computer security training to Bureau area and agency offices and other organizations such as schools. Additionally, a 1996 contractor-performed risk assessment recommended that the system security function be moved from the Center and elevated organizationally, but the recommendation had not been implemented at the time of our current audit.

Regarding Recommendation A.2, our prior audit found that the security implementation plan for the Bureau's automated information systems for fiscal year 1996 was not documented. Although a security implementation plan was prepared by November 1996 (for fiscal year 1997), the plan did not meet the detailed requirements of Office of Management and Budget Circular A- 130, Appendix III, "Security of Federal Automated Information Resources." The plan addressed the security needs of the Bureau, but the plan did not address the security needs of the Office of the Special Trustee or include specific steps to meet the security needs of the Bureau and the Office of the Special Trustee, thus ensuring that an adequate security program was in place for the automated systems of the Bureau and the Office of the Special Trustee. The Bureau did not have an adequate security program because the Bureau reported that "virtually no security planning" had occurred because of the downsizing of the Office of Information Resources Management. We also found that Bureau management did not assess the effectiveness of the Bureau's system security program as part of its annual review under the Federal Managers' Financial Integrity Act.

In its response to the prior audit report, the Bureau stated, as part of its reorganization and redescription of the Office of Information Resources Management, that "the position of Security Officer will be elevated to report directly to the Director of OIRM [Office of Information Resources Management]." In addition, the Bureau concurred "with respect to those functions which will remain the responsibility of the Bureau subsequent to the transfer of mainframe data processing to the U. S.G. S. [Geological Survey]" and that the development

of the policies and procedures would be the responsibility of the Bureau IT Security Manager, who would complete them by October 1, 1997. Bureau management agreed to provide the security staff with the authority to implement and enforce a Bureauwide system security program but did not agree to provide additional staff to meet the responsibilities. The Bureau stated that "[t]he recommendation would be appropriate if the Bureau were to continue to operate mainframe data processing," but that the data processing "function will be transferred to U.S.G.S. [Geological Survey], [and]. . . the Bureau Security Officer and his staff will be able to manage the reduced security requirements of the Albuquerque OIRM [Office of Information Resources Management] site."

Our followup review found that the IT Security Manager continued to report to the Acting Chief of the Center and that the IT Security Manager had not (1) developed new or revised policies and procedures for a Bureauwide system security program, (2) implemented and enforced a security program, and (3) evaluated the effectiveness of the security program. The Departmental Manual (375 DM 19) states:

Bureau IT Security Manager is responsible for: managing the bureau IT security program, coordinating all bureau activities designed to protect IT resources, coordinating bureau IT security training programs, and reporting on the effectiveness of these activities to the bureau and Departmental management.

Additionally, Office of Management and Budget Circular A- 130, Appendix III, requires that controls over general support and major application systems be reviewed every 3 years or more frequently if significant changes are made to the systems or risks are determined to be high.³ Further, the IT Security Manager position description included these responsibilities. However, Bureau management had not held the IT Security Manager accountable for performing these duties.

The Center was performing data processing functions and serving as a general support system, since it will continue to control the operating system, security software, and application processing for the IBM applications; operate and run a Unisys computer and applications; and operate as a network management center. We believe that the need for Bureauwide system security planning, implementation, and training and for system security oversight will not diminish but will increase and be more complex. Without a system security program, Bureau management has little assurance that its existing system security is operating effectively. Additionally, the Bureau will not be in compliance with Office of Management and Budget Circular A-l 30, Appendix III, because an adequate system security

communications network, [and] a departmental data processing center including its operating system and utilities."

³Office of Management and Budget Circular A- 130, Appendix III, "Security of Federal Automated Information Resources," defines a general support system as "an interconnected set of information resources under the same direct management control which shares common functionality." The Circular further states that a general support system "normally includes hardware, software, information, data, applications, communications and people" and that examples of a system are a local area network, ...an agency-wide backbone, a

program was not in place and the system security program had not been evaluated for its effectiveness during the past 3 years. We consider these recommendations not implemented because Bureau management did not (1) elevate the IT Security Manager function to report directly to the Chief, Office of Information Resources Management; (2) hold the IT Security Manager accountable for performing position description responsibilities; and (3) ensure that the Bureau had an effective system security program. Further, we believe that once a security program is implemented, Bureau management should ensure that an evaluation of the effectiveness of the program is performed periodically and that the Bureau includes any resultant corrective actions in future Bureau security plans.

Recommendation A.3. The Bureau's security personnel perform risk assessments of the Bureau's automated information systems environment and as appropriate, provide assurance that the necessary changes are implemented to manage the risks identified.

Recommendation C. 1. The Bureau develop and implement policies to classify the Bureau's computer resources in accordance with the results of Periodic risk assessments and guidance contained in Office of Management and Budget Circular A- 130, Appendix III.

Regarding Recommendation A.3, our prior audit found that risk assessments had not been performed periodically or that they had not been performed when systems, facilities, or other conditions changed. Specifically, since 1990, only two risk assessments had been performed. These assessments were of the Center's previous mainframe configuration in 1990 and the local area networks of the Albuquerque Central Offices in 1996. While we determined that these assessments were adequate, none of the recommendations from the risk assessments had been implemented. Regarding Recommendation C. 1, we found that Bureau management had not classified its computer resources, such as data files, application programs, and computer-related facilities and equipment. Resource classification allows management to (1) determine the level of security that should be provided to protect against unauthorized modification, disclosure, loss, or impairment and (2) determine whether security controls should be implemented or document Bureau management's acceptance of the risk.

In its response to the prior audit report, the Bureau stated that "the FY [fiscal year] 1996 reduction-in-force eliminated OIRM [Office of Information Resources Management] staffs capability to perform risk assessments [and resource classifications]." The Bureau further stated that "from the resources freed as a result of the transfer of data processing and as part of the reorganization/redescription..., positions will be established to perform the necessary risk assessments [and resource classifications]." The Bureau also stated that the risk assessments and classifications "will commence in July 1998" and "will be completed within 18 months of that date."

We agreed with the Bureau's statement that commencement of risk assessments and resource classifications could be performed by resources that will become available as a result of transferring data processing functions to the Geological Survey. However, since the Bureau's response to the prior audit report, the then Chief, Office of Information Resources Management, retired, and the position had not been filled by the end of fiscal year 1997. Consequently, Bureau management had not developed and implemented its

reorganization/redescription for the Office of Information Resources Management. Further, we found that Center personnel had not become available to perform the assessments and classifications because the Center had not transferred all of its data processing responsibilities to the Geological Survey and was continuing to function as a general support system. In addition, Bureau management had not approved an information technology strategic plan for the Center to provide direction following the consolidation with the Geological Survey's host computer. Further, all of the owners of the Bureau's automated information system resources could not be identified. Therefore, we believe that the risk assessment and resource classification reviews cannot be performed in the time fiame identified in the Bureau's response, Accordingly, we consider these recommendations not implemented. We believe that Bureau management should redetermine when the Bureau can begin performing its risk assessments and resource classifications.

Recommendation B. 1. Ensure that personnel security Policies and Procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel in sensitive or critical ADP [automated data processing1 positions and for informing the security staff. in writing, whenever employees who are system users terminate their employment or are transferred.

Recommendation E. 1. Ensure that Policies are developed and implemented which match personnel files with system users periodically, that user IDs are deleted from the system for users whose employment has been terminated. and that verification and approval are obtained from users' supervisors and application owners or managers that the levels of access are appropriate.

Regarding Recommendation B. 1, our prior audit found that personnel in sensitive or critical ADP positions, such as system and application programmers, including application programmers not assigned to the Center, did not have documented background investigations for security clearances or did not have security clearances at a level commensurate with their positions. In addition, we found that, although the IBM computer had been set to automatically revoke a user identification (ID) after 180 days of inactivity, supervisors did not notify the application owner or manager or the Center's security staff to revoke and delete a user ID when an employee's employment was terminated or when an employee was transferred. Regarding Recommendation E. 1, we found that IT security staff and application owners did not periodically review user access authorizations to ensure that the levels of access to computer resources were appropriate.

Regarding Recommendation B.1, the Bureau stated in its response to the prior audit report that "The necessary information will be submitted to the Office of Personnel Management to conduct/update the clearances of the Operations Service Center staff by June 1, 1997." In addition, the Bureau stated that actions will be taken to provide a report monthly to the Office of Information Resources Management which identifies employees who transferred within the Bureau and employees whose employment was terminated so that system access can be reviewed and modified or revoked.

Regarding Recommendation E. 1, the Bureau stated that the action taken to implement this recommendation was the transfer of the mainframe data processing to the Geological Survey's host computer and that December 1, 1997, was the target date for the completion of the transfer. In addition, we accepted the action to be taken by the Bureau for Recommendation B. 1, to provide a monthly report to the Office of Information Resources Management, as appropriate to partially implement Recommendation E. 1.

Our followup audit found that policies and procedures were not developed, implemented, and enforced for ensuring that (1) appropriate security clearances for personnel in sensitive or critical ADP positions were obtained, (2) security staff was informed whenever employees who were system users terminated their employment or were transferred, (3) security clearances had not been updated for all Bureau employees who filled sensitive or critical ADP positions except for 14 of the 55 Center employees who filled such positions, and (4) users' levels of access were reviewed and validated periodically. The "Generally Accepted Principles and Practices for Securing Information Technology Systems," issued by the National Institute of Standards and Technology, recommends that reviews and validation of the appropriateness of users' levels of access be performed periodically and, if necessary, the users' access be modified or revoked. Although reports were to be produced monthly that were to identify employees who had transferred within the Bureau or employees who had terminated their employment, Bureau management had not ensured that the reports were provided to the Bureau's IT security management staff. Additionally, we found that the agreement between the Bureau and the Geological Survey did not include provisions for the Geological Survey to ensure that users' levels of access were properly authorized and were appropriate for the users to perform their day-to-day duties or that access would be validated periodically for the Bureau's IBM applications.

Accordingly, we consider Recommendation B. 1 partially implemented and Recommendation E. 1 not implemented. Additionally, Bureau management should ensure that personnel who are not assigned to the Center and who are in sensitive or critical ADP positions have security clearances commensurate to the positions held. Further, if Bureau management does not require Bureau personnel to review and validate the appropriateness of users' levels of access to the Bureau's IBM applications, the agreement between the Bureau and the Geological Survey should be modified to include the requirement that the Geological Survey perform periodic reviews and validate the appropriateness of users' levels of access to the Bureau's IBM applications.

Recommendation D.1. Sufficient staff are provided to adequately monitor all visitor activities.

Recommendation D.2. Funding is provided for adequate maintenance of the commuter operations room. such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room.

Our prior audit found that the Center was located within a Federal building that provides unauthorized individuals access to the Center. To ensure that the Center and its resources were safeguarded, physical access to the Center was achieved by electronic key cards and monitored by video cameras. However, custodial (contractor) personnel and building managers were provided key cards, which afforded an opportunity for uncontrolled access to the Center. Additionally, we found that general housekeeping and maintenance of the computer operations room were performed only weekly. This weekly schedule was not adequate because of the failure to remove potential fire hazards, such as combustible supplies and dust produced by paper used in the printer, that were housed in the computer operations room.

In its response to the prior audit report, the Bureau stated, "The action taken to implement these recommendations is the conversion of the mainframe data processing to the U.S.G.S. [Geological Survey] host computer."

Our followup audit found that, while the Bureau may no longer house the IBM and Unisys mainframe computers in the computer operations room, a clean and well-maintained computer operations room was still needed. The computer operations room housed server computers and telecommunications equipment for the Bureau's wide area network and the Albuquerque Central Office's local area networks. We found that custodial staff and building managers continued to have access to this sensitive area and that the room was cleaned only weekly. In addition, the printers and other combustible supplies remained in the room. Further, physical hazards, such as file cabinets placed in front of printers, existed for personnel who operated and maintained the computer equipment and peripherals. Therefore, we consider these recommendations not implemented.

Recommendation F. 1. Ensure that a higher priority is given to moving the applications that reside on the Unisys mainframe to the IBM mainframe.

Our prior audit found that passwords were not changed periodically and inactive user IDs were not automatically revoked on the Unisys computer. Additionally, greater reliance had to be placed on the user ID and password controls to protect the applications, files, and data because the applications residing on the Unisys computer were developed without access controls and could not be modified to install the access controls. Therefore, these controls were inadequate. However, the Bureau and the Office of the Special Trustee were planning to move the applications residing on the Unisys mainframe to the IBM mainframe.

In its response to the prior audit, the Bureau stated that it would transfer the data processing functions to the Geological Survey's host computer.

Our followup audit found that the applications which resided on the Unisys mainframe were not converted to the Bureau's IBM mainframe; therefore, the Unisys applications could not be moved to the Geological Survey's host computer. The Unisys applications could not be converted because of the lack of documented programs and because of the antiquated programming language used for the Unisys applications. The contractor estimated the cost to convert the applications to be in excess of \$1 million. However, as an interim solution, the Department's Office of Information Resources Management approved the Bureau's acquisition of a Unisys server computer. The applications would be moved from the Unisys mainframe to the Unisys server. The Department's Office of Information Resources

Management stated that the Bureau should continue to convert these applications to operate on an IBM mainframe computer. In our opinion, because the Office of the Special Trustee was redeveloping its applications that reside on the Unisys server computer, the Unisys applications should not be converted to the Geological Survey's host computer, as originally recommended, but be maintained on the Unisys server until the Office of the Special Trustee's redevelopment project is completed. This action could save the Bureau at least \$1 million in conversion costs. We believe that the Bureau should not implement the original recommendation because of the costs involved in converting the Unisys applications. Accordingly, we consider the recommendation resolved because it is no longer applicable.

Recommendation G. 1. Ensure that Policies and procedures are developed and implemented which clearly identify the individuals responsible and accountable for application development and changes.

Our prior audit found that the software development and change controls were inadequate to ensure that the proper version of an application was used in production. Based on our test of the National Irrigation Information Management System, we found that the application programmers not only programmed the application but also tested, authorized, and approved the movement of the modified programs from test or development into production. In addition, the lead programmer was not notified of software modifications. Further, one member of the Center's systems staff, who was a programmer, could move application software changes from test or development into production without the approval of the lead programmer.

In its response to the prior report, the Bureau stated that the Office of Information Resources Management was "in the process of expanding and documenting improved procedures in this area" and that the target date for completion was July 1, 1997.

Our followup audit found that new or revised policies and procedures related to application development and changes were not developed and that individuals had not been assigned responsibilities for application development or changes. Because the policies and procedures had not been developed and responsibility had not been assigned, controls for application software development and change had not improved. For the National Irrigation Information Management System, the application programmers continued to test applications and to approve the movement of the modified programs into production without the knowledge of the lead programmer. For the Loan Management and Accounting System, the application developer did not fully document change requests or modifications to the System. In addition, the Loan Management and Accounting System application developer had full access to user passwords and the loan databases. Further, Center personnel and contractors were developing client/server applications without any documented Bureau management support. Accordingly, we consider this recommendation not implemented.

Recommendation H. 1. Ensure that staffing at the Center is evaluated and adjusted so that duties for critical system support functions are adeauately segregated and fully utilized.

Recommendation I. 1. Ensure that access and activities of the Center's system programmers are controlled and monitored by security staff and that Resource Access Control Facility (RACF) controls are established to Protect system resources.⁴

Regarding Recommendation H.1, our prior audit found that the duties for the support functions of system design, application programming, systems programming, quality assurance/testing, library management, change management, data control, data security, and data administration were not adequately segregated between different individuals.

Regarding Recommendation I. 1, we found that controls established over system software were not effective in detecting and deterring inappropriate use. Specifically, periodic reviews of the System Maintenance Facility logs and RACF access reports were not performed by the security staff to monitor system activities effectively. Additionally, the security staff produced reports that identified users and the computer resources accessed; however, the staff had not produced or used the primary "auditing" or monitoring reports that could be used to provide oversight of system activities. One system programmer had "alter" access to system software, the System Maintenance Facility logs, and RACF logs, which provided an opportunity for the programmer to alter his activities, as well as those of other users. Thus, the audit trails of system activities could be impaired or destroyed. Further, the RACF could be used to establish controls and monitor access to the computer resources, but it had not been set up to effectively control access to the system resources. We found that one of the "start procedures" could bypass all verification processing, including the security classification checks, and therefore affect the overall security of the system. Further, RACF was not used to protect critical system resources, including the system parameter library, linklist libraries, master catalog, and the primary and backup files. Finally, no logging or audit trails were available.

In its response to the prior audit report, the Bureau stated that it will implement these recommendations through the "conversion of the mainframe data processing" to the Geological Survey's host computer.

Our followup audit found that Center management had not segregated system functions and had not changed the use of the RACF to be an effective critical resource control. Specifically, functions such as systems design, application programming, systems programming, quality assurance/testing, library management, change management, data control, data security, and data administration had not been segregated between different individuals. Further, one system programmer continued to have "alter" access to system software, the System Maintenance Facility logs, and RACF logs. Because the Center will continue to maintain control over the IBM operating system and security software at the Geological Survey's host computer through at least fiscal year 1998 and will continue to

Resource Access Control Facility **(RACF)** is an IBM-licensed software security product that protects information by controlling access to the information. RACF provides security by identifying and **verifying** users to the system, authorizing users' access to protected resources, and recording and reporting access attempts. (<u>Resource Access Control Facility General Users Guide, Version 1. Release 9.2</u>, 9th edition, IBM Corp., 1993, page 1-1.)

operate Unisys applications, the need for segregation of duties between different individuals and the use of RACF controls to protect system resources still exists. Accordingly, we consider these recommendations not implemented.

Recommendation J.1. Ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility.

Our prior audit found that the Center did not have an effective means to recover or to resume computer operations in the event of a system failure or a disaster. The Center was developing a service continuity plan for fiscal year 1997. The off-site storage facility was not located at least 1 mile from the Center, and the facility did not adequately safeguard information and data stored from unauthorized access and environmental hazards such as heat and humidity. Thus, the data stored were at risk of loss or damage.

In its response to the prior audit report, the Bureau stated, "To ensure service continuity in case of system failure or a disaster, the Office of Information Resources Management (OIRM) has a contract for back-up of it's a-17 [Unisys] computer." The Bureau further stated, "OIRM has determined that a similar contract for its IBM 3090 computer is not warranted because of the pending transfer to the U.S. Geological Survey (USGS) of the data processing operation." The Geological Survey had indicated that it had a contract which would cover the Bureau's systems during the transfer to the host computer. The Bureau did not specifically respond to the recommendation on acquiring a secure off-site storage facility.

Our followup audit found that the Bureau did have a contract and, in a test situation, had successfully recovered its Unisys applications. However, the Bureau had not acquired an environmentally sound and secure off-site storage location. As such, the backup tapes were stored on-site in the Center's computer room. Accordingly, we consider the recommendation partially implemented.

Recommendations

We recommend that the Assistant Secretary for Indian Affairs ensure that the Bureau of Indian Affairs:

- 1. Establishes as a high priority the use of the Geological Survey's host computer's operating, security, and automated job scheduling systems.
- 2. Develops and approves an Office of Information Resources Management strategic plan which provides direction to and defines the functions of the Operations Service Center.
- 3. Holds the IT Security Manager accountable for performing the position responsibilities.
- 4. Performs periodically an evaluation of the system security program's effectiveness and includes any resultant corrective actions in future Bureau security plans.

- 5. Redetermines, based on the Office of Information Resources Management's strategic plan, when the Bureau can begin performing risk assessments and classifying its resources. Also, personnel who will be responsible for the risk assessments and resource classifications should be identified.
- 6. Obtains security clearances for ADP personnel who are not assigned to the Center that are commensurate with their positions.
- 7. Requires Bureau staff to review and validate the appropriateness of users' levels of access to the Bureau's IBM applications. If the users' levels of access are not reviewed and validated by Bureau personnel, the Bureau should modify its agreement with the Geological Survey to include the requirements that access reviews and verifications be performed for the IBM applications by the Geological Survey.
 - 8. Removes all safety hazards from the computer operations room.

Bureau of Indian Affairs Response and Office of Inspector General Reply

In the May 19, 1998, response (Appendix 2) from the Assistant Secretary for Indian Affairs to this audit report, the Bureau concurred with Recommendations 1, 2, 3, 4, 5, 6, and 7 and concurred "in part" with Recommendation 8. Based on the response, we consider Recommendations 1 and 8 resolved and implemented and Recommendations 2, 3, 4, 5, and 6 resolved but not implemented. Accordingly, the unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation. Also based on the response, the Bureau is requested to provide additional information for Recommendation 7 (see Appendix 3).

Regarding our April 1997 report, the Bureau in its May 1998 response, concurred with Recommendations A. 1, A.2, A.3, B. 1, C. 1, E. 1, G. 1, H. 1, I. 1, and J. 1 and concurred in part with Recommendations D. 1 and D.2. Based on the response, we consider Recommendations A. 1, D. 1, I. 1, and J. 1 resolved and implemented and Recommendations A.2, A.3, B. 1, C. 1, D. 1, E. 1, G. 1, and H. 1 resolved but not implemented (see Appendix 4). Accordingly, this information on the prior recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget.

In accordance with the Departmental Manual (360 DM 5.3), we are requesting a written response to this report by July 10, 1998. The response should provide the information requested in Appendix 3.

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Bureau personnel in the conduct of our audit.

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR AUDIT REPORT "GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, OPERATIONS SERVICE CENTER, BUREAU OF INDIAN AFFAIRS"

Status of Recommendations and Corrective Actions

Recommendations

A.1. The information technology security function is elevated organizationally to at least report directly to the Director, Office of Information Resources Management; is formally provided with authority to implement and enforce a Bureauwide system security program; and is provided staff to perform the required duties, such as providing computer security awareness training and performing periodic risk assessments.

Not implemented. Bureau management had not reorganized the Office of Information Resources Management to elevate the information technology security function to report directly to the Director, Office of Information Resources Management. Bureau management also had not ensured that the information technology security function was provided with authority to implement and enforce a Bureauwide system security program. In its response, Bureau officials stated that the staff would not be increased because of the transfer of data processing functions to the Geological Survey, which has not occurred.

A.2. A system security program is developed and documented which includes the information required by the Computer Security Act of 1987 and Office of Management and Budget Circular A-1 30, Appendix III, and that policies and procedures are implemented to keep the system security program current.

Not implemented. A revised system security program and new or revised policies and procedures had not been developed, and an evaluation of the security program's effectiveness had not been performed.

A.3. The Bureau's security personnel perform risk assessments of the Bureau's automated information systems environment and, as appropriate, provide assurance that the necessary changes are implemented to manage the risks identified.

Not implemented. Corrective actions to implement the recommendation, such as the reorganization of the Office of Information Resources Management and the transfer of data processing functions to the Geological Survey, had not occurred.

B. 1 Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel in sensitive or critical ADP positions and for informing the security staff, in writing, whenever employees who are system users terminate their employment or are transferred.

Partially implemented. No new or revised personnel security policies and procedures had been developed. Although the necessary paperwork to initiate security clearances for 14 Center employees had been prepared, security clearance paperwork had not been initiated for employees who were not assigned to the Center and performed ADP sensitive and critical functions. Also, Bureau management was to provide the security staff with monthly reports that identified Bureau personnel who had terminated their employment or who were transferred; however, the reports had not been provided to the security staff.

C.1. Develop and implement policies to classify the Bureau's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A- 130, Appendix III.

Not implemented. No new or revised policies had been developed. Additionally, Bureau management had not taken corrective actions, such as reorganizing the Office of Information Resources Management and transferring data processing functions.

D. 1. Sufficient staff are provided to adequately monitor all visitor activities.

Not implemented. Corrective actions were dependent upon transferring data processing functions to the Geological Survey, which had not occurred. However, the Center had installed server computers and network communications equipment that also required safeguarding.

D.2. Funding is provided for adequate maintenance of the computer operating room, such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room.

Not implemented. Corrective actions were dependent upon data processing functions being transferred to the Geological Survey, which had not occurred. However, the Center had installed server computers and telecommunications equipment in the computer operations room, which also needed to be protected from dust and fire hazards.

E.1. Ensure that policies are developed and implemented which match personnel files with system users periodically, that user IDs are deleted from the system for users whose employment had been terminated, and that verification and approval are obtained from user supervisors and application owners or managers that the levels of access are appropriate.

Not implemented. No new or revised policies had been developed. Additionally, Bureau management was to provide the security staff with monthly reports identifying Bureau personnel who had terminated their employment or who were transferred; however, the reports had not been provided to the security staff. Additionally, Bureau management's corrective action was dependent upon transferring data processing functions to the However, data Geological Survey. processing functions were not transferred, and the agreement between the Bureau and the Geological Survey did not contain provisions for the Geological Survey to ensure that users' levels of access were properly authorized and were appropriate for the users to perform their day-to-day duties or that the access would be validated periodically.

- F. 1. Ensure that a higher priority is given to moving the applications that reside on the Unisys mainframe to the IBM mainframe.
- Resolved. The recommendation is no longer applicable.
- G. 1. Ensure that policies and procedures are developed and implemented which clearly identify the individuals responsible and accountable for application development and changes.

Not implemented. No new or revised policies had been developed.

H.1. Ensure that staffing at the Center is evaluated and adjusted so that duties for critical system support functions are adequately segregated and fully utilized.

Not implemented. Corrective actions were dependent upon data processing functions being transferred to the Geological Survey. However, for at least fiscal year 1998, the Bureau will continue to operate and control the IBM operating system and security software after the transfer to the Geological Survey. Additionally, the Bureau will be operating and controlling a Unisys server computer and maintaining the applications that will reside on the Unisys computer.

I. 1. Ensure that access and activities of the Center's system programmer are controlled and monitored by security staff and that RACF controls are established to protect system resources.

Not implemented. Corrective actions were dependent upon data processing functions being transferred to the Geological Survey. However, for at least fiscal year 1998, the Bureau will continue to operate and control the IBM operating system and security software.

J.1. Ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility.

Partially implemented. Although a contingency plan had not been developed, the Bureau had contracted for a backup site for the Unisys mainframe computer in the event of a disaster and had tested the functionality of the backup site. Additionally, the Geological Survey had agreed to include the Bureau's operating system and security and application software as part of the Geological Survey's contingency plan. However, Bureau management had not acquired a secure offsite storage facility for the data and files.



United States Department of the Interior

OFFICE OF THE SECRETARY Washington, D.C. 20240

MAY 1 9 1998

Memorandum

To: Assistant Inspector General for Audits

From: Assistant Secretary - Indian Affairs June Manue

Subject: Draft Audit Report on Followup of General Controls Over Automated Information

Systems, Operations Service Center, Bureau of Indian Affairs (A-IN-BIA-00 1-97)

The subject audit report addresses the Bureau of Indian Affairs (Bureau) implementation of the recommendations made by the Office of Inspector General in its April 1997 audit report entitled "General Controls Over Automated Information Systems_ Operations Service Center, Bureau of Indian Affairs" (Report No. 97-I-771). The followup audit found that the Bureau had partially implemented 2 of the 13 recommendations made in the April 1997 report and had not implemented 10 recommendations and that 1 recommendation was no longer applicable. The audit concluded that the general control risks identified by the prior audit for fiscal year 1996 continued to exist during fiscal year 1997. The subject audit report includes eight new recommendations.

The Bureau generally agrees with the findings of the followup audit. As noted in our response to the April 1997 audit, the Office of Information Resources Management was to undergo a reorganization and redescription of positions because of the transfer of mainframe data processing from the Bureau to the U.S. Geological Survey. Although the reorganization/ redescription began in fiscal year 1997, the resignation of the Director and the transfer and subsequent retirement of the Deputy Director limited its effectiveness. The reorganization is well underway, and the Acting Director, Office of Information Resources Management is on-site in Albuquerque, New Mexico. As discussed below, the Service Center has taken actions to implement many of the recommendations and to improve its controls. Finally, the Bureau appreciates the changes made to the draft report from our discussions on the preliminary draft report.

As requested, we have provided a revised corrective action plan for the unimplemented recommendations. To avoid repeating corrective actions, we have included the new recommendations with the unimplemented recommendations from the prior audit.

Followup Audit Recommendation 1. We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs establishes as a high priority the use of the Geological Survey's host computer's operating, security, and automated job scheduling functions.

Bureau Response. The Bureau concurs. The Service Center will complete the transfer of all IBM mainframe operations, system software support, and security administration functions to the U.S. Geological Survey Data Center in Reston, Virginia. by May 3 1, 1998. We consider this recommendation implemented.

Followup Audit Recommendation 2. We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs develops and approves an Office of Information Resources Management strategic plan which provides direction to and defines the functions of the Operations Service Center.

Bureau Response. The Bureau concurs. A comprehensive strategic plan for the Office of Information Resources Management is being developed and finalized under contract with **MitreTek**. The strategic plan will be completed by September 30, 1998. The responsible official is the Director, **Office** of Information Resources Management.

Prior Audit Recommendation A.1. The information technology security function be elevated organizationally to at least report directly to the Director, Office of Information Resources Management; is formally provided with authority to implement and enforce a Bureauwide system security program; and is provided staff to perform the required duties, such as providing computer security awareness training and performing periodic risk assessments.

Followup Audit Recommendation 3. We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs holds the IT Security Manager accountable for performing the position responsibilities.

Bureau Response. The Bureau concurs. The **Information** Technology Security Manager's position has reported to the Office Director since October 1997. (See Attachment 1.) The position has Bureauwide authority for the information technology security program. As noted in our response to the prior report, we believe that **sufficient** staff will be available to manage the security requirements once we transfer the remaining processing functions for the IBM computer to the Geological Survey. As with all employees, Bureau management will hold the Security Manager accountable through the performance appraisal process. The reorganization will be completed by September 30, 1998. The responsible official is the Director, **Office** of Information Resources Management.

Prior Audit Recommendation A.2. A system security program is developed and documented which includes the information required by the Computer Security Act of 1987 and Office of Management and Budget Circular A-130, Appendix III, and that policies and procedures are implemented to keep the system security program current.

Followup Audit Recommendation 4. We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs performs periodically an evaluation of the system security program's effectiveness and includes any resultant corrective actions in future Bureau security plans.

Bureau Response. The Bureau concurs. The Bureau has entered into an agreement with Washington Administrative Service Center- West to develop a comprehensive computer security plan

that will address computer security policies, operating procedures, responsibilities, contingency planning and risk analysis. (See Attachment 2.) The plan will be developed in accordance with the standards and guidance published in the Office of Management and Budget Circular A-130; the National Institute of Standards and Technology's Federal Information Processing Standards Publications dealing with automated information system security; and the Office of Personnel Management's Federal Personnel Manual issuances on personal security as they relate to automated information systems. The plan's operating procedures and the management control reviews required by the Department's Office of Information Management will ensure that the plan be periodically reviewed and updated. The plan will be developed by July 3 1, 1998. The responsible official is the Information Technology Security Manager.

Prior Audit Recommendation A.3. The Bureau's security personnel perform risk assessments of the Bureau's automated information systems environment and, as appropriate, provide assurance that the necessary changes are implemented to manage the risks identified.

Prior Audit Recommendation C.I. Develop and implement policies to classify the Bureau's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A- 130, Appendix III.

Followup Audit Recommendation 5. We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs redetermines, based on the Office of Information Resources Management's strategic plan when the Bureau can begin performing risk assessments and classifying its resources. Also, personnel who will be responsible for risk assessments resource classifications should be identified.

Bureau Response. The Bureau concurs. Risk assessments and classifications of the Bureau's automated information systems environment will be performed beginning in fiscal year 1999 in accordance with the Bureau's security program plan. The Information Technology Security Management staff will provide oversight of this effort. Risk assessments and classifications will be done by teams consisting of personnel from the Bureau's Office of Information Resources Management and the program offices.

Prior Audit Recommendation B.1. Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel in sensitive or critical ADP positions and for informing the security staff, in writing, whenever employees who are system users terminate their employment or are transferred.

Prior Audit Recommendation E.I. Ensure that policies are developed and implemented which match personnel files with system users periodically, that user ID(s) are deleted from the system for users whose employment has been terminated, and that verification and approval are obtained from user supervisors and application owners or managers that the levels of access are appropriate.

Followup Audit Recommendation 6. We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs obtains security clearances for ADP personnel who are not assigned to the Center that are commensurate with their positions.

Followup Audit Recommendation 7. We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs requires Bureau staff to review and validate the appropriateness of users' levels of access to the Bureau's IBM applications. If the users' levels of access are not reviewed and validated by Bureau personnel, the Bureau should modify its agreement with the Geological Survey to include the requirements that access reviews and verifications be performed for the IBM applications by the Geological Survey.

Bureau Response. The Bureau concurs. In February 1998, the Bureau reorganized its position sensitivity and security program. As part of this effort, the Central Office is reviewing all sensitive positions, including information technology positions, to determine whether the positions are classified consistently. Once the position descriptions are reviewed, the personnel system will be updated and a listing generated that will identity individuals needing initial and upgraded investigations or reinvestigations. While we will complete this initial effort by September 30, 1998, the scheduling of the investigations will be dependent on available area office funding. The Bureau's Security Officer, however, will monitor the area offices to ensure that the investigations are completed. In addition, the Information Technology Security Manager will ensure that the employee termination report is received and reconciled with system users. The report will also be provided to the Geological Survey for its use in managing Bureau system user profiles.

Prior Audit Recommendation D.l. Sufficient staff are provided to adequately monitor all visitor activities.

Prior Audit Recommendation D.2. Funding is provided for adequate maintenance of the computer operating room, such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room.

Followup Audit Recommendation 8. We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs removes all safety hazards from the computer room.

Bureau Response. The Bureau concurs in part. We believe that we have implemented these recommendations to the extent possible given our available resources. Monitoring of visitor activities is handled by the organizational element receiving the visitor(s). All non-Service Center personnel must register with the Information Technology Security Manager. A minimum number of access keys have been provided to custodial, building security, and GSA building managers based upon their need to enter the facility. In addition, the Service Center has funded full time housekeeping and maintenance service for the computer room and ancillary facilities beginning in fiscal year 1998. Finally, the Service Center has corrected the safety deficiencies identified by the Division of Safety Management in its annual safety and health evaluation for fiscal year 1997.

Prior Audit Recommendation G.1. Ensure that policies and procedures are developed and implemented which clearly identify the individuals responsible and accountable for application development and changes.

Bureau Response. The Bureau concurs. The Bureau recruited and filled the Chief, Applications Support Branch, position in November 1997. The Branch is developing and implementing standards,

procedures, and policies to ensure **full** accountability for all application system change management and production implementation of the Office's applications. This guidance, when finalized, will be distributed to all Bureau offices which develop and/or maintain application systems. The responsible official is the Chief, Applications Support Branch.

Prior Audit Recommendation H.l. Ensure that staffing at the Center is evaluated and adjusted so that duties for critical system support functions are adequately segregated and fully utilized.

Prior Audit Recommendation 1.1. Ensure that access and activities of the Center's system programers are controlled and monitored by security **staff** and that Resource Access Control Facility (RACF) controls are established to protect system resources.

Bureau Response. The Bureau concurs. This has been accomplished for the applications residing on the IBM computer with the transfer of the remaining application operations system software support, and security functions to the Geological Survey. The operating system and security features of the new Unisys NX Server provide much improved safeguards for the data and applications residing on this platform. Although RACF controls are not compatible with the Unisys NX Server, the Bureau will establish similar controls. Finally, separation of duties, to the extent possible, was considered during the reorganization/redescription of positions for the Service Center. We consider these recommendations implemented.

Prior Audit Recommendation J.1. Ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility.

Bureau Response. The Bureau concurs. As stated in the draft audit report, the Bureau has a disaster recovery contract that has been fully tested and certified for the Unisys hosted applications. In addition, the Bureau has obtained off-site storage for its backup media at the Southwestern Indian Polytechnic Institute which is approximately 8 miles from the Service Center. We consider this recommendation implemented.

Attachments



United States Department of the Interior

BUREAU OF INDIAN AFFAIRS Information Resources Management Operations Service Center 500 Gold Avenue, S.W. P.O. Box 888 Albuquerque, New Mexico 87103

Office of Information Resources Management Operations Service Center MS-611

FEB - 3 1998

MEMORANDUM

REPLY TO

ATTN OF: Acting Director, Office of Information Resources Management

SUBJECT: Bureau AIS Security Officer Status.

TO: Acting Director, Management and Administration

In **accordance** with the recommendation of the Department Inspector **General**, **Position** Number **K00283-01223**, **GS-0334-13**, Computer Specialist within our Operations Service Center, **has** reported directly to the undersigned since October 26, **1997**.

This position is encumbered by Jerry K. Belew, who is currently designated the BIA

Automated Information Systems (AIS) Security Administrator.

George Cover

Acting Director, OIRM

CC

Personnel office, Albuquerque Area Office Jerry **Fiely**, Deputy Director - Audit & Evaluation

APPENDIX 2 Page 7 of 9

WASC-West Project Scope Statement
March 1998
Revised March 10, 1998

Project Number 98-053

Project Title

Development of Security Plan

Client

BIA

Program Manager

Tony Manzi, WASC-West

Project Leader

Ellen Erikson

Project Team

WASC:

Jim Opeka

USGS:

Blanche Heard

BIA:

Jerry Belew; Lorraine Jaramillo; Wesley Anderson

Project Description

Problem Statement

The Bureau of Indian Affairs (BIA) has identified the need to develop a comprehensive computer security plan. The plan will address computer security policies, operating procedures, responsibilities, contingency planning, and risk analysis. The plan should be developed in accordance with the standards and guidance published in the Office of Management and Budget (OMB) Circular No. A-130; the National Institute of Standards and Technology's Federal Information Processing Standards Publications (FIPS PUBS) dealing with automated information system security; and the Office of Personnel Management's Federal Personnel Manual issuances on personal security as they relate to automated information systems.

Background

BIA recently transferred its mainframe computer applications **from** Albuquerque, NM to the U.S. Geological Survey (USGS) **mainframe** computer in **Reston**, VA The applications are currently operating in a separate partition of the USGS **mainframe**. BIA is responsible for administering security for these applications. There are still a number of BIA applications running on hardware located in Albuquerque, NM. BIA **staff is also** responsible for security at the Albuquerque installation.

In addition, the Office of the Inspector General issued a draft audit report (A-IN-BIA-

WASC-West Project Scope Statement
March 1998
Revived March 10, 1998

001-97) in February 1998, that identifies a number of issues and recommendations relative to computer security.

The proposed security plan needs to address security policies, standards, and procedures that are applicable to the current operating environment, consistent with applicable USGS policies and procedures, and responsive to the recommendations in the **draft** audit report.

Project Objectives

The objective of this project is to develop a comprehensive computer security program that:

- complies with applicable Federal regulations and guidelines,
- provides an appropriate response to the OIG draft audit report, and
- ensures that BIA hardware, software, and application data is secure.

The computer security program will address the following:

- security policies, standards, and operating procedures,
- administrative, physical, application., and personal security,
- individual and organizational security responsibilities,
- contingency and disaster recovery planning,
- risk analysis policies and procedures.

Target Deliverable Dates

March 20, 1998	Proposed Project Scope Statement delivered to BIA	
April 3, 1998	Proposed Project Scope Statement approved by BIA	
April 10, 1998	Detailed project plan delivered to BIA	
May 29, 1998	Draft security plan delivered to BIA	
June 19, 1998	Draft security plan approved by BIA	
July 3, 1998	Fii security plan delivered to BIA	
July 10, 1998	Proposal for implementing security plan delivered to BIA (if	
•	requested)	

Project Methodology

General Approach

A project team will be established that includes representation **from BIA**, the WASC, and USGS. The team will review appropriate Federal guidelines and regulations, interview applicable computer personnel, inventory BIA applications residing in **Reston** and Albuquerque, review applicable USGS computer security plans, and review the OIG draft report findings and recommendations. The project leader will provide periodic project status updates to the WASC-West program manager who in turn will provide updates to

WASC- West Project Scope Statement
M-arch 1998
Revised March 10, 1998

BIA management. Policy and procedures issues will be brought to BIA management for resolution as required.

Assumptions

BIA applications currently operating in a separate partition of the USGS mainframe computer will eventually migrate to the general production area of the mainframe and **RACF** security for BIA will be integrated into the regular production **RACF** security database.

Mainframe computer security administration will eventually be the responsibility of USGS personnel.

At least one member of the project team will be familiar with the BIA Unisys system applications and access controls.

STATUS OF CURRENT AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	status	Action Required
land8	Implemented.	No further action is required.
2, 3, 4, 5 , and 6	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
7	Management concurs; additional information needed.	Provide target dates for when (1) the IT Security Manager will begin receiving the employee termination reports and (2) the supervisors and application owners will begin approving levels of access. Additionally, a copy of the modified agreement with the Geological Survey requiring access reviews and verifications should be provided to the Office of Inspector General.

STATUS OF PRIOR AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	status	Action Required
A.1, D.1, I.1, and J.1	Implemented	No further action required.
A.2, A.3, B.1, C.1, D.1, E.1, G.1, and H.1	Resolved, not implemented	No further response to the Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

ILLEGAL OR WASTEFUL ACTMTIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

Within the Continental United States

U. S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240

Our 24-hour Telephone HOTLINE 1-800-424-508 1 or (202) 208-5300

TDD for hearing impaired (202) 208-2420 or 1-800-354-0996

Outside the Continental United States

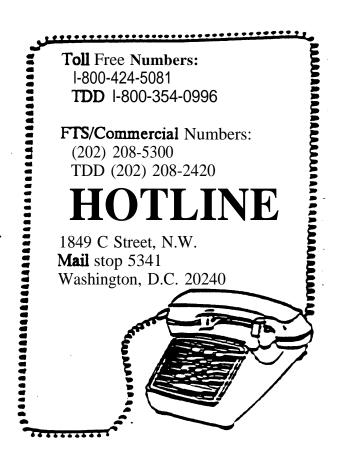
Caribbean Region

U.S. Department of the Interior Office of Inspector General Eastern Division - Investigations 4040 Fairfax Drive Suite 303 Arlington, Virginia 22201

(703) 235-9221

North Pacific Region

U.S. Department of the Interior Office of Inspector General North Pacific Region 415 Chalan San Antonio Baltej Pavilion, Suite 306 Tamuning, Guam 96911 (67 1) 647-605 1





U.S. Department of the Interior Office of Inspector General

AUDIT REPORT

FOLLOWUP OF MAINFRAME COMPUTER
POLICIES AND PROCEDURES,
ADMINISTRATIVE SERVICE CENTER,
BUREAU OF RECLAMATION

REPORT NO. 98-I-623 AUGUST 1998



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

AUG 20 1998

AUDIT REPORT

Memorandum

To: Commissioner, Bureau of Reclamation

Robert J. Williams Pokert J. Williams
Assistant Inspector General for Audits From:

Audit Report on Follow-up of Mainframe Computer Policies and Procedures, Subject:

Administrative Service Center, Bureau of Reclamation (No. 98-I-623)

INTRODUCTION

This report presents the results of our followup audit of recommendations contained in our March 1997 audit report "Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation" (No. 97-I-683). We performed this audit in support of audits of the annual financial statements of the Bureau of Reclamation and the Service Center's clients. Annual financial statements are required by the Chief Financial Officers Act. The objective of this audit was to determine whether (1) the Service Center had satisfactorily implemented the recommendations made in our prior audit report and whether any new recommendations were warranted and (2) the Service Center's general controls were effective over computer center management and operations, software change management, and mainframe computer operating system software.

BACKGROUND

The Bureau of Reclamation's Administrative Service Center in Denver, Colorado, is one of two Administrative Service Centers within the Department of the Interior. The Service Center's mission "is to improve economy and efficiency in Government through the delivery of standard. automated administrative systems." Specifically, the Service Center provides (1) consolidated payroll and personnel services for about 97,000 employees in the Department of the Interior and eight other Federal agencies and (2) Government accounting, integrated budgeting, and reporting services through the Federal Financial System (FFS) to three Departmental and five other Federal agencies. At the time of our audit, payroll and personnel services were provided through the Payroll/Personnel System (PAY/PERS) and the Federal Personnel Payroll System (FPPS) that was in the latter stages of development. The implementation of FPPS, which is to replace PAY/PERS, began in September 1997 with the conversion of three Departmental agencies from PAY/PERS. The remaining Departmental and non-Departmental agencies are to be converted to FPPS by December 30,

1998. In addition, a new client, the Social Security Administration, was added in March 1998, which increased the number of payroll accounts by about 65,000.

The Service Center provides its services on a cost-reimbursable basis, and this reimbursement function is administered through the Bureau's Working Capital Fund. The Service Center is organized into seven divisions that "provide data center, application, system, and operational support to the organization and clients" as follows:

- The ADP Services Division is responsible for (1) planning, developing, and operating the Service Center's computer center functions and (2) operating and maintaining computers, system software, and data communication networks. To assist the Division in carrying out its functions, the Service Center has contracted with Tri-Cor Industries, Inc. The Division provides data processing support for the Departmental standardized administrative sensitive systems.' To support these systems, the computer center operates an IBM mainframe computer using the "OS/390" operating system to manage the processing work load. The access control security software installed on the mainframe computer is the Resource Access Control Facility (RACF), which controls users' and computer programs' access to the mainframe computer resources. Additionally, other system software, such as database management, telecommunications, and specialized vendor software, reside on the mainframe computer and are used to support the sensitive systems. Data center operations provide users with computer and communications equipment and infrastructure, systems software, and operational support. The Division manages data center operations through scheduling activities, planning for contingencies and capacity, and providing user support. The Division also manages the information resources security program.
- The FPPS Division is responsible for managing the development, implementation, and operation of the FPPS application. These responsibilities include controlling software changes; providing technical assistance to users; and managing tests of the application, converting data, and implementing the FPPS application. To assist the Division in carrying out its functions, the Service Center has contracted with the Computer Sciences Corporation.
- The Application Management Office directs the program activities of the Departmental administrative applications assigned to the Service Center.
- The PAY/PERS Division operates and maintains PAY/PERS. However, when all agencies have been converted to FPPS, the PAY/PERS Division will no longer exist.

^{&#}x27;According to the National Institute of Standards and Technology, sensitive systems are defined as "systems that contain any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

²RACF is an IBM-licensed product that provides access control by identifying and verifying users to the system, authorizing access to protected resources, logging detected accesses to protected resources, and logging detected unauthorized attempts to enter the system.

- The Payroll Operations Division plans, develops, executes, and manages the interagency payroll program delivered by the Service Center and performs payroll administration and services for all payroll clients.
- The Financial Systems Division provides functional and technical support to clients using FFS and related financial applications.
- The Management Services Division provides Service Center administrative support.

SCOPE OF AUDIT

The scope of our followup audit included an evaluation of the actions taken by Service Center management to implement the 24 recommendations made in our March 1997 audit report and a review of the general controls in place during fiscal year 1997. To accomplish our objective, we interviewed Service Center and contractor personnel, reviewed systems documentation, observed and became familiar with computer center operations, analyzed system security, reviewed system and application software maintenance procedures, and reviewed and tested implementation of the prior audit recommendations. Because our review was limited to evaluating the adequacy of internal controls at the Service Center, we did not test the effectiveness of the internal controls at the various agencies and clients supported by the Service Center.

Our audit was conducted in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we evaluated the Service Center's general controls over its mainframe computer and application systems that could adversely affect the data processing environment. The control weaknesses that we identified are summarized in the Results of Audit section and discussed further in Appendix 1 of this report. If implemented, our recommendations should improve the general controls in the areas cited. Because of inherent limitations in any system of internal controls, losses, noncompliance, or misstatements may occur and not be detected. We also caution that projecting our evaluations to future periods is subject to the risk that controls or the degree of compliance with the controls may diminish.

PRIOR AUDIT COVERAGE

During the past 5 years, the General Accounting Office has not issued any reports related to the scope of this audit. However, the Office of Inspector General has issued two related reports as follows:

- The March 1994 audit report "Compliance With the Computer Security Act of 1987, Denver Administrative Service Center, Bureau of Reclamation" (No.94-I-3 57) stated that the Service Center generally complied with the requirements of the Computer Security Act of 1987 but that improvements were needed in the areas of security and operations. Since the Service Center was addressing all of the deficiencies identified, the report contained no recommendations
- The March 1997 audit report "Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation" (No.97-I-683) stated that deficiencies identified in our March 1994 report relating to performing a risk analysis of the Service Center's local area networks and separating duties by using RACF security software still existed. This report contained 24 recommendations for improving management and internal controls at the Service Center. We reviewed actions taken by Service Center management to implement these recommendations as part of our current audit, the results of which are summarized in the Results of Audit section and discussed in Appendix 2 of this report.

RESULTS OF AUDIT

Regarding the prior report's recommendations, we found that the Bureau of Reclamation's Administrative Service Center management had satisfactorily implemented 21 of the 24 recommendations (see Appendix 2). Of the three remaining recommendations, one recommendation (No. D.3) was scheduled for completion by September 30, 1998, and we considered the planned actions adequate to correct the deficiencies identified. We considered the remaining two recommendations (Nos. G.2 and J.l) partially implemented because actions had not been completed to fully correct the previously identified deficiencies. The actions taken to implement the 2 1 recommendations have improved the controls in the areas of local area network protection; application access; mainframe system physical and logical security; and contingency planning, backup, and disaster recovery.

Regarding the general controls, we believe that overall, the general controls were operating with no material weaknesses. However, we found general control weaknesses in the areas of computer center management and operations, software change management, and mainframe computer operating system software that were present during fiscal year 1997. Office of Management and Budget Circular A-130, "Management of Federal Information Resources," which defines minimal sets of controls for managing Federal information resources, and National Institute of Standards and Technology publications require Federal agencies to establish and implement computer security and management and internal controls to improve the protection of sensitive information in the computer systems of executive branch agencies. Additionally, the Congress has enacted laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls is adequate. Also, the Departmental Manual outlines (1) the requirements related to security clearance programs, suitability, and types of security investigations and (2) the process for determining position sensitivity. However,

Service Center management did not ensure that controls were implemented and were operating effectively and in compliance with established criteria. Specifically, we found that general control practices and processes were not complied with, the appropriate security levels were not assigned to automated data processing (ADP)-related positions, some mainframe computer functions were not operated efficiently, software change management controls were not complied with, and mainframe computer operating system software tools and settings had not been implemented to ensure system and data integrity. As a result, there was an increased risk of unauthorized access to, modification of, and disclosure of client-sensitive data; inefficient Service Center operations; and loss of system and data integrity.

Overall, we identified 6 weaknesses and made 14 recommendations for improving the general controls at the Service Center. The weaknesses in the areas of computer center management and operations, software change management controls, and mainframe computer operating system software are discussed in the following paragraphs, and details of the weaknesses and our respective recommendations to correct these weaknesses are in Appendix 1.

Computer Center Management and Operations

We found that Government and contractor employees who filled ADP-related sensitive and critical positions did not have proper background clearances. Without information on the security-related background of personnel assigned to sensitive and critical positions, there was an increased risk that sensitive systems could be impaired or compromised. In addition, Service Center operations could be improved if some mainframe computer functions, such as moving changed software from the test environment to the production environment process and scheduling computer production, were centralized, and a standardized software change control tool was used. When mainframe computer functions are decentralized and not standardized, there is an increased risk of inefficient operations and unnecessary costs. We made three recommendations to address these weaknesses.

Software Change Management Controls

We found control weaknesses in the area of managing software changes made to the FPPS application and to the mainframe computer operating system. Because of the weak controls, there was an increased risk that unauthorized changes could be made to the sensitive FPPS application and to the critical operating system, which could affect application and system integrity. We made seven recommendations to address these weaknesses.

Mainframe Computer Operating System Software

We found that the Service Center had not implemented the available operating system software tools which would improve (1) the effectiveness of access controls to the mainframe computer resources and (2) mainframe computer system processing and data integrity. As a result, the risk was increased that access controls could be bypassed and unauthorized

activities would not be detected. We made four recommendations to address the weaknesses in this area.

Bureau of Reclamation Response and Office of Inspector General Reply

In the June 17, 1998, response (Appendix 3) to the draft report from the Commissioner, Bureau of Reclamation, the Bureau concurred with all 14 of the new recommendations. Based on the response, we consider Recommendations C. 1 and C.2 resolved and implemented and Recommendations A. 1, A.2, B. 1, C.3, D. 1, D.2, D.3, D.4, E. 1, E.2, F. 1, and F.2 resolved but not implemented. Accordingly, the unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (see Appendix 4).

In its response, the Bureau said that "the report language regarding the FPPS system did not adequately consider that FPPS was under development during the time of the audit." We disagree. We clearly identified in Finding C that the weaknesses occurred during the latter stages of development and the early stages of implementation. However, we have added wording (page 1) to further clarify that the FPPS was in the latter stages of development during the period of our review.

Regarding our March 1997 report, we consider 2 1 recommendations resolved and implemented and the remaining 3 recommendations (Nos. D.3, G.2, and J.1) partially implemented. Accordingly, updated information on the status of the three prior recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget (see Appendix 5).

Since the recommendations contained in this report are considered resolved, no further response to the Office of Inspector General is required (see Appendix 4).

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Bureau personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

COMPUTER CENTER MANAGEMENT AND OPERATIONS

A. Background Clearances

Condition: In our prior report, we recommended that Service Center management require all contractor employees to have proper background clearances. However, during our current audit, we found that contractor personnel at the ADP Services Division had received background clearances but that not all contractor personnel at the FPPS and Financial Systems Divisions had received background clearances. Additionally, Service Center Federal personnel involved in designing, developing, operating, or maintaining sensitive automated systems did not have background checks and security clearances commensurate with their job responsibilities and the sensitivity of the information accessed. Specifically, 154 of the 189 Service Center employees who performed these ADP-related duties did not have the appropriate ADP background clearances.

Criteria:

Office of Management and Budget Circular A- 130, Appendix III, "Security of Federal Automated Information Resources," requires agencies to establish and manage security policies, standards, and procedures that include requirements for screening individuals participating in the design, development, operation, or maintenance of sensitive applications or those having access to sensitive data. In addition, the Departmental Manual (441 DM 4.6) requires position sensitivity levels of "non-critical sensitive" or "critical sensitive" and associated security clearances for ADP-related positions for which employees are required to design, test, operate, and maintain sensitive computer systems. Security clearances are also required of employees who have access to or process sensitive data requiring protection under the Privacy Act of 1974. Further, the Departmental Manual (441 DM 5.15) requires that all consultants or contractors performing ADP-related sensitive and critical duties have background investigations to determine position suitability and to receive a security clearance.

Cause:

Service Center management had not uniformly developed and implemented, across all Service Center Divisions, personnel security policies requiring contractor personnel who perform ADP-related sensitive and critical duties to

be screened for position suitability. Additionally, Service Center management did not ensure that the level of position sensitivity for ADP-related positions was assigned at the level commensurate with the risk and sensitivity of the data accessed and processed and that background checks were performed on employees who filled these positions.

Effect:

Without proper personnel background investigations, managers had limited knowledge of the suitability of their employees and contractors, from a security standpoint, for their respective jobs. Without this assurance, there was an increased risk that the Service Center's sensitive systems could be impaired or compromised by personnel.

Recommendations

We recommend that the Director, Administrative Service Center:

- 1. Develop and implement policies and procedures which require contractor employees who fill ADP-related sensitive or critical positions to have documented suitability screening and proper background investigations and appropriate security clearances.
- 2. Evaluate the position sensitivity of ADP-related positions, assign position sensitivity levels in accordance with the Departmental Manual, and ensure that those employees working on sensitive systems have the proper background investigations and security clearances before they are assigned to the positions.

B. Operating Efficiencies

Condition: At the Service Center, each division controlled the process of moving changed

software from the test to the production environment, different software tools were used to control the movement of the changed software, and internal and external clients controlled their mainframe computer production scheduling.

Criteria: Office of Management and Budget Circular A-1 30 states that management

should oversee its processes to maximize return on investment and minimize financial and operational risk. Further, the Circular requires that financial management systems conform to the requirements of Office of Management and Budget Circular A- 127, "Financial Management Systems." Circular A- 127 requires that agency financial management systems process financial events

effectively and efficiently.

Cause: Service Center management did not ensure that its processes were operating

efficiently because of preferences of internal and external clients and because management had not developed and implemented consistent standards for

controlling operational processes.

Effect: There was an increased risk that changed software would negatively impact the

mainframe computer operating system; costs of maintaining different software tools would increase Service Center operating costs, which would be passed on to clients; and mainframe computer usage could be reduced. Additionally, without centralized control of production scheduling, there was an increased

risk that critical processing jobs would not receive the required priority.

Recommendation:

We recommend that the Director, Administrative Service Center, in coordination with the Service Center's internal and external clients, evaluate the feasibility of centralizing the process of moving changed software from the test environment to the production environment, using standardized software tools to control the software change process, and centralizing mainframe computer production scheduling.

C. Application Software Change Management Controls

Condition: Software changes made to the FPPS during the latter stages of development and the early stages of implementation were not approved, reviewed, or evaluated adequately before changed software was installed for use in production; documentation was not adequate to monitor changes made to the software; and available library control software' was not implemented to ensure consistency and completeness throughout the FPPS application.

Criteria:

Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," provides guidelines for managing software Publication 106 states that all software changes should be maintenance. carefully evaluated and formally reviewed prior to installing the changed software. The publication further states, "In order to monitor maintenance effectively, all activities must be documented. ... The key to successful documentation is that not only must the necessary information be recorded, it must be easily and quickly retrievable by the maintainer." In addition, FPPS Division policies and procedures require that all changes to the FPPS application be thoroughly documented, be accepted by all involved parties, and pass a quality assurance review.

Cause:

FPPS Division management did not ensure that Division personnel followed software change management practices for making software changes to the FPPS application because of the time constraints to implement FPPS and because FPPS was encountering problems and was considered by Division personnel to be unstable. In addition, we found that FPPS Division management did not hold its personnel accountable for complying with Division policies and procedures when they made changes to the FPPS Further, FPPS Division management said that they did not implement the available library control software, which would ensure adequate documentation of the FPPS application, because at that time, the vendor library control software was not working correctly.

Effect:

There was an increased risk that the changes made to the FPPS application would not perform according to specifications, which could adversely affect user satisfaction and could adversely impact other applications interfacing with the FPPS application or the mainframe operating system.

^{&#}x27;Library control software is a system for keeping track of changes to and versions of software programs, documenting components to build executable programs, and preventing unauthorized access to program files.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Require that software changes be adequately reviewed and approved before the changes are implemented.
- 2. Implement procedures to ensure that all software changes to the FPPS application are properly documented.
- 3. Implement the available library control software when corrected to ensure adequate documentation of the FPPS application.

D. Operating System Software Change Management

Condition: Change controls over the mainframe computer operating system software were not adequate. The ADP Services Division change control procedures did not address adequate separation of duties between the development, test, and installation functions. Thus, one individual could perform all of these critical functions. In addition, the change control procedures did not ensure that all changes were properly approved by Division management. While the change management procedures required approval of all software changes, changes were made without documented evidence of approval.

Criteria:

Appendix III of Office of Management and Budget Circular A-1 30 states that one of the minimum controls required in a general support system is personnel controls. One such control is separation of duties, which is "the practice of dividing the steps in a critical function among different individuals." Also, Federal Information Processing Standards Publication 106 states that "to be effective, the policy should be consistently applied and must be supported and promulgated by upper management to the extent that it establishes an organizational commitment to software maintenance." In addition, Publication 106 states that "prior to installation, each change (correction, update, or enhancement) to a system should be formally reviewed." Finally, Division system change request procedures require that all change requests be approved by the appropriate branch chief.

Cause:

ADP Services Division management did not ensure that appropriate separation of duties existed in developing and testing mainframe operating system software and parameter changes and in moving operating system software and parameter changes into the production environment, although the number of employees within the Division may allow for a separation of these duties. Additionally, Division management had not implemented controls to ensure that the process of making system software changes was in compliance with its documented procedures. Further, management had not implemented procedures to require periodic reviews of critical datasets and system parameters to identify inappropriate changes to the mainframe operating system environment. Although Division management had implemented a change control software tool that provided a systematic and automated means of controlling the movement of software changes, all the capabilities of the software tool were not implemented because of other Division priorities.

Effect:

There was an increased risk that unauthorized, untested, and undocumented changes could be made to the mainframe computer operating system software and parameters, which would affect system processing and data integrity, and that these changes would not be detected or detected in a timely manner.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Evaluate current ADP Services Division procedures and determine the feasibility of implementing controls in the change management process over operating system software to ensure that adequate separation of duties is addressed and complied with.
- 2. Develop procedures and implement controls to ensure that changes to the operating system parameters are identified, approved by ADP Services Division management, and documented.
- 3. Develop procedures requiring periodic reviews of critical datasets and system parameters.
- 4. Evaluate implementing available capabilities in the current change control software tool to more effectively control changes to the operating system software.

E. System Audit Tools

a 1141 a

Condition: Service Center management did not use available mainframe computer operating system audit tools that would improve integrity over system processing and data and that would detect inappropriate actions by authorized users. Specifically:

- Operating system integrity verification and audit software was not used. Such software could assist data center and installation security management in identifying and controlling the mainframe computer operating system's security exposures that may result from system setting options; from installing "back doors" to the operating system; and from introducing viruses and Trojan horses, which can destroy production dependability and circumvent existing security measures.
- Computer operators and system programmers had the capability to change the system initialization process and thus affect system processing. System options that would log the results in the SYSLOG² of actions taken by the computer operators and system programmers affecting mainframe operating system configuration were not implemented. Therefore, an audit trail of the system initialization process and changes to the operating system configuration could not be produced for periodic review. Based on recommendations made by our audit staff during the review, Service Center management implemented the logging capabilities within the system; however, procedures had not been developed and implemented to require periodic reviews of the logs.
- Periodic reviews of critical System Management Facility (SMF)³ logs to identify unauthorized changes to data by authorized users and critical events affecting system processing were not performed. For example, reviews were not performed of record type 7, which records when the system audit trail is lost, and record type 90, which records events such as SET TIME, SET DATE, and SET SMF, all of which affect system processing and audit trails.

²SY SLOG is an audit trail that logs the results of actions taken by computer operators and system programmers during system initialization.

³The System Management Facility (SMF) logs record all system activity and serve as an audit trail of system activity, including identifying users who performed the activity.

Criteria:

Appendix III of Office of Management and Budget Circular A-1 30 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, the Circular states that individual accountability is one of the personnel controls required in a general support system. The Circular further states that an example of one of the controls to ensure individual accountability includes reviewing or looking at patterns of users' behavior, which requires periodic reviews of the audit trails. Also, the National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" states that audit trails are "technical mechanisms" to achieve individual accountability.

Cause:

Service Center management did not acquire operating system integrity and verification software, did not encourage the use of available system audit trails to detect and identify inappropriate actions affecting the system processing and data integrity, and did not establish procedures requiring periodic reviews of available system logs. Instead, Service Center management relied on its staff to make appropriate changes to the system initialization process and on authorized users to make only appropriate changes.

Effect:

As a result, there was an increased risk that mainframe computer operating system security exposures would not be identified. Additionally, without periodic reviews of the system audit trails, there was an increased risk that processing problems or unauthorized activities would not be detected or detected timely and that the responsible individuals would not be held accountable for the inappropriate actions.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Evaluate acquiring system verification and auditing software.
- 2. Develop and implement procedures to ensure that periodic reviews are performed of the SYSLOG and critical SMF logs to identify unauthorized or inappropriate activities and that unauthorized or inappropriate activities are reported to Service Center management.

F. Mainframe Operating System Options

Condition: ADP Services Division management did not implement mainframe operating system options that would strengthen controls over computer programs which access sensitive operating system functions. We found 13 libraries that were able to run in the "Authorized Program Facility (APF)-authorized" state, even though the libraries were not required to run in the APF. By running in the APF-authorized state, these libraries may be considered part of the main&me operating system and thus have access to all of the mainframe resources.

Criteria:

IBM's publication titled "OS/390 Initialization and Tuning Reference" states that "the parameter LNKAUTH specifies whether all libraries" in the LNKLST** member? "are to be treated as Authorized Program Facility (APF)authorized when accessed as part of the concatenation, or whether only those libraries that are named in the APF table are to be treated as APF-authorized? Additionally, the publication addresses managing system security and states that the "authorized program facility (APF) allows your installation to identify system or user programs that can use sensitive system functions."

Cause:

Division Management implemented a default option (LNKLST) that allowed libraries within the LNKLST** member to run in the APF-authorized state. An alternative option (APFTAB) is provided which requires only those libraries that are named specifically in the APF table to be able to run in the APFauthorized state. The 13 libraries were automatically added to the LNKLST** member when the operating system was upgraded in July 1997. Because Division management did not review the members used to define APFauthorized libraries, these 13 libraries remained in the LNKLST** member.

⁴A library is a collection of programs or data files or a collection of functions (subroutines) that are linked into the main program when it is compiled. (The Computer Language Company, Inc., Computer Desktop Encyclopedia, Version 9.4, 4th Quarter, 1996.)

^{&#}x27;Concatenation means to link together in a series or chain. (Webster's Ninth New Collegiate Dictionary, Merriam-Webster Inc., Springfield, Massachusetts, 1989, p. 27 1.)

⁶LNKLST** member "defines the collection of program libraries to be searched, in sequence, for programs when no specific [library] has been supplied in the job stream." (Mark S. Hahn, CONSUL Risk Management, Inc., A Guide to SYS1 PARMLIB, Monograph Series 4, The Information Systems Audit and Control Foundation, Inc., Rolling Meadows, Illinois, February 1996, p. 38.)

Further, because Division management implemented the LNKLST option, these 13 libraries were unnecessarily provided the ability to run in the APF-authorized state. Therefore, management did not have assurance that only approved libraries had access to sensitive operating system functions. Based on recommendations of our audit staff during the review, the libraries were removed from the LNKLST** member. However, if the APFTAB option had been used, Division personnel would have been required to enter the 13 library names into the APF table, thus providing additional assurance that only approved libraries would run in the APF-authorized state.

Effect:

By implementing the LNKLST option rather than the APFTAB option, the risk increased for unauthorized libraries to run in an authorized state, thus bypassing operating system controls, and for system integrity to be lost.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Evaluate the feasibility of using the APFTAB option, thus providing additional assurance that only approved libraries would run in the APF-authorized state.
- 2. Perform periodic reviews of all members used to define the APF-authorized libraries to ensure that only those required to run in the APF-authorized state are given this authority.

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR AUDIT REPORT "MAINFRAME COMPUTER POLICIES AND PROCEDURES, DENVER ADMINISTRATIVE SERVICE CENTER, BUREAU OF RECLAMATION" (No. 97-I-683)

ъ			. •	
Reco	mm	end	atıc	ns

Status of Recommendations and Corrective Actions

A. 1. Require all contractor employees to have proper background clearances.

Implemented. All contractor employees in the ADP Services Division are required to have background clearances. However, the current review found that contractor employees in other Service Center Divisions did not have appropriate clearances.

B.l. Enhance the intruder detection settings to suspend a user account, after unsuccessful access attempts, for a period of time long enough to ensure that the user will have to contact an administrator to have the user ID reset.

Implemented. NetWare intruder lockout settings have been modified on all production servers to suspend a user identification (ID) for a period of 24 hours after three incorrect log-in attempts have been made within a 24-hour period.

Cl. Develop and periodically update a disaster recovery plan for the LAN.

Implemented. Subsequent to the completion of current fieldwork, the LAN Disaster recovery Plan was completed.

D.1. Ensure that LAN security and password features are implemented which will require all users to change passwords every 90 days; enforce unique password use; and limit concurrent multiple or unlimited connections to one per user and grant additional connections on an asneeded basis.

Implemented. The password change interval has been revised to 90 days or less on all servers. Unique passwords are required for all individual users. Concurrent multiple connection authority has been removed from all accounts except for those where a demonstrated need exists.

D.2. Include the "SECURE CONSOLE" command in the AUTOEXEC.NCF file on all file servers to prevent users from gaining access to the system files in DOS mode.

Implemented. A procedure to secure the console on all Service Center file servers was implemented. At the monitor console screen, the "LOCK FILE SERVER CONSOLE OPTION" was implemented to lock the system console manually whenever the server is initialized.

Status of Recommendations and Corrective Actions

Recommendations

D.3. Ensure that the command "SET Partially implemented. ALLOW UNENCRYPTED PASSWORD=ON" is not present in the AUTOEXEC.NCF file.

All Service Center NetWare servers will be configured to require encrypted passwords when all Service Center NetWare file servers have been migrated to NetWare Directory Services. This is 75 percent implemented. The target date for full implementation originally was March 31, 1998, but the date has been changed to September 30, 1998.

Service Center users' access to the "least privileged" in the FFS application; that is, assurance should be provided that any user authorized to enter or change the vendor table does not also have access to disbursing documents.

E.l. Coordinate with the client to limit Implemented. As requested by the Service Center, the client has changed FFS security so that no employee has access to both vendor tables and disbursement documents.

F. 1. **Document** procedures for the issuance of key cards and require that the procedures be instituted for vendors in addition to contractors and Federal employees.

Implemented. Procedures for the issuance of card keys for vendors, contractors, and Federal employees have been documented.

outside of the ADP Services Division to be issued permanent card keys because such access should be limited to those individuals performing their day-to-day duties.

F.2. Evaluate the need for individuals Implemented. The evaluation has been completed. Permanent card keys are issued to only those individuals deemed appropriate.

Status of Recommendations and Corrective Actions

Recommendations

F.3. Document procedures to ensure the Service Center's compliance with the Information Systems Handbook regarding visitor (such as maintenance personnel, janitorial staff, and vendors) monitoring.

Implemented. Procedures for monitoring visitor access to the computer room have been Department of the Interior Automated documented in compliance with the Departmental Handbook.

G. 1. Evaluate the feasibility of setting the parameters in RACF security software to require one numeric or special character as part of the password, as recommended by the Bureau's Security Administrator.

Implemented. Evaluation of using one numeric or special character as part of the Service Center standard password has been completed. Service Center management, in coordination with its clients, determined that requiring numeric or special characters as part of the password was not feasible.

G.2. Reevaluate the standard RACF password change intervals and revocation settings to ensure that the level of risk associated with the mainframe applications and the current password settings is acceptable to the Service Center, as well as to its clients and the Department, and address the results in a current risk assessment.

Partially implemented. The Service Center issued a memorandum to the system owners in October 1997 outlining the alternatives identified in the feasibility study referenced in Recommendation G. 1. System owners responded in December 1997, agreeing to reduce the expiration period for passwords from 180 days to 90 days, reduce the allowable period of inactivity of a user ID from 180 days to 90 days, and remove inactive user IDs from the system after 1 year of inactivity. With the exception of one client, all inactive users are removed manually once a month. Procedures for removing Social Security inactive users are being developed.

H. 1. Evaluate the feasibility of limiting the number of Service Center users who have access authority to alter SMF logs.

Implemented. Evaluation has been completed. This authority has been limited to three seniorlevel system programmers who work in the System Software Management Branch.

Recommendations

Status of Recommendations and Corrective Actions

H.2. Ensure that the SMF record type 60 logging is active or RACF settings are adjusted to specifically audit critical datasets maintained on the mainframe computers and to therefore provide an audit trail of system activity.

Implemented. Batch and TSO type 60 records are written to the SMF log. Type 60 record collection has been activated for "started tasks" as well.

I. 1. Evaluate the extent to which the "OPERATIONS" attribute should be available to Service Center user IDs. Specifically, the use of other more restrictive RACF authorities (such as DASDVOL authority) should be considered where possible.

Implemented. Evaluation has been completed. Assignment of the OPERATIONS attribute has been restricted to employees who need the attribute to perform their duties.

1.2. Activate the security feature RACF OPERAUDIT and ensure that security personnel perform periodic reviews of the resultant logs to identify unauthorized activity.

Implemented. The feature OPERAUDIT has been activated, and the resultant logs will be reviewed on a quarterly basis by the Service Center Computer Security Manager.

J. 1. Ensure that the group responsible for monitoring security performs periodic reviews of user access levels to identify required necessary changes and to ensure that user access levels are authorized. Partially implemented. The identification of critical datasets has been completed, and a requirement to perform periodic reviews of reports auditing the critical datasets has been established. Performance of these actions would enable monitoring personnel to identify user access levels; however, the actions would not ensure that the user access level was authorized. Therefore, procedures need to be established to compare the critical dataset reports with approved user authorization requests.

Recommendations

Status of Recommendations and Corrective Actions

5.2. Institute a policy of "least privileged" access levels to ensure that access to resources and data is limited to those users who require such access.

Implemented. A policy of "least privileged" access is in place.

K. 1. Evaluate the staffing requirements of the group responsible for monitoring security to ensure the separation of duties within RACF. Implemented. The ADP Services Division has completed the evaluation and has identified adequate staffing within the Division for accomplishing the separation of the security administration and auditing functions. The security administration function will be maintained with the same staffing levels. The security auditing function will be placed within a quality management function in the Division's IRM and Customer Service Branch.

L. 1. Document and implement procedures to ensure that Decentralized Security Administration Facility records are updated for oral access adjustments to allow for the reconciliation of access requested with access allowed.

Implemented. While the Bureau disagreed with the recommendation, it has taken action to modify existing policy and procedures to reflect a new process.

M. 1. Provide resources to ensure the development of a computer security plan for the sensitive systems in accordance with the Computer Security Act and Management. Circular A- 130, Appendix III.

Implemented. A computer security plan for 1997 was developed and submitted to the Department of the Interior's Office of Information Resources Management.

N. 1. Perform a risk analysis of the Service Implemented. A risk analysis of the computer Center's computer center and its center has been completed. applications.

	Status of Recommendations and
Recommendations	Corrective Actions



United States Department of the Interior

BUREAU OF RECLAMATION

Washington, D.C. 20240

D-5010 ADM-8.00 JUN 17 1998

JUN 18 AC

Memorandum

To:

Office of Inspector General

Attention: Robert J. Williams, Acting Inspector General

From:

Eluid L. Martinez

Commissioner

Subject:

Draft Audit Report on Followup of Mainframe Computer Policies and Procedures,

Administrative Service Center, Bureau of Reclamation

(Assignment No. A-IN-BOR-00 1-97)

As required by Departmental Manual 360 DM 5.3, attached is the Bureau of Reclamation's written response to the subject audit report of our mainframe computer operations at the Denver Administrative Service Center (ASC). The schedule proposed for implementation of some of the recommendations recognizes the ASC's existing commitment to the complete implementation of the Federal Personnel Payroll System (FPPS) by the end of calendar year 1998.

While we generally support the audit recommendations, some of the discussion in the report is misleading and should be clarified. The report language regarding the **FPPS** system did not adequately consider that FPPS was under development during the time of the audit. According to the **draft** report, the period of audit coverage was fiscal year 1997. The **FPPS** was still in a development mode at that time, and there is a considerable difference between a **software** project in the development mode versus the maintenance mode. Some of the report language (e.g., page 10 of the draft report) could lead a reader to believe that FPPS is presently an unstable system. This is not true and should be clarified before the report is issued in final form.

We appreciate the opportunity to comment on the audit recommendations and anticipate working with your office towards a constructive resolution. If you have any questions or concerns, please contact Stan **D**UM, Administrative Service Center Director, at (303) 969-7200.

Attachment

cc. Assistant Secretary - Water and Science, Attention: Carla Burzyk (w/ attachment)

OIG Draft Report "Followup of Mainframe Computer Policies and Procedures, Administrative Service Center"

COMPUTER CENTER MANAGEMENT AND OPERATIONS

A. Background Clearance-s

Condition: In our prior report, we recommended that Service Center management require all contractor employees to have proper background clearances. However, during our current audit, we found that contractor personnel at the ADP Services Division had received background clearances but that not all contractor personnel at the **FPPS** and Financial Systems Divisions had received background clearances. Additionally, Service Center Federal personnel involved in designing, developing, operating, or maintaining sensitive automated systems did not have background checks and security clearances commensurate with their job responsibilities and the sensitivity of the information accessed. **Specifically**, 154 of the 189 Service Center employees who performed these ADP-related duties did not have the appropriate ADP background clearances.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires agencies to establish and manage security policies, standards, and procedures that include requirements for screening individuals participating in the design, development, operation, or maintenance of sensitive applications or those having access to sensitive data. In addition' the Departmental Manual (441 DM 4.6) requires position sensitivity levels of "non-critical sensitive" or "critical sensitive" and associated security clearances for **ADP-related** positions for which employees are required to design, test, operate, and maintain sensitive computer systems. Security clearances are also required of employees who have access to or process sensitive data requiring protection under the Privacy Act of 1974. Further, the Departmental Manual (441 DM 5.15) requires that all consultants or contractors performing ADP-related sensitive and critical duties have background investigations to determine position suitability and to receive a security clearance.

Cause:

Service Center management had not uniformly developed and implemented, across all Service Center Divisions, personnel security policies requiring contractor personnel who perform ADP-related sensitive and critical duties to be screened for position suitability. Additionally, Service Center management did not ensure that the level of position sensitivity for ADP-related positions was assigned at the level commensurate with the risk and sensitivity of the data accessed and processed and that background checks were performed on employees who filled these positions.

Effect:

Without proper personnel background investigations, managers had limited knowledge of the suitability of their employees and contractors, from a security standpoint, for their respective jobs. Without this assurance, there was an increased risk that the Service Center's sensitive systems could be impaired or compromised by personnel.

Recommendations

We recommend that the Director, Administrative Service Center:

1. Develop and implement policies and procedures which require contractor employees who fill ADP-related sensitive or critical positions to have documented suitability screening and proper background investigations and appropriate security clearances.

Response

Concur. The Denver Administrative Service Center (ASC) will develop and distribute policy to all affected ASC offices regarding security clearances and background investigations for contractor personnel. The policy will be distributed by October 1, 1998. In addition, the ASC will review and amend as necessary all personnel contracts to include the requirement for background investigations and security clearances for existing and future contract personnel by January 1, 1999. The responsible official is the Chief, Applications Management Office.

There are two types of contractual service arrangements at the ASC. Some employees work under a third-party contract with other agencies, usually the General Services Administration (GSA). In these cases, the servicing agency contract controls all contractual requirements and clauses. The requesting agency (ASC) may outline additional security requirements in the task order statement of work as long as the additional requirements are within the parameters of the original contract. All GSA contractors in both the ADP Services and Financial Systems Division were subject to background security investigations through GSA's requirements and procedures. These investigations were completed as.of May 1997. As of March 1998, the Federal Personnel Payroll System (FPPS) Program Management Division contractor employees changed from a Department of the Army contract to a GSA contract. As a result of the preliminary audit findings, ASC security requirements were added to the task order under the GSA contract.

Another type of contractual arrangement is a direct contract between the ASC and the service contractor. All current direct contracts either already have the proper security clauses or will have the proper clauses by January 1, 1999, to comply with security requirements. All existing and future contractual service agreements will be reviewed to ensure compliance with the requirements for background security checks.

2. Evaluate the position sensitivity of ADP-related positions, assign position sensitivity levels in accordance with the Departmental Manual, and ensure that those employees working on sensitive systems have the proper background investigations and security clearances before they are assigned to the positions.

25

Response

Concur. The ASC will review ADP-related positions in the ASC organizations to **verify** the appropriate requirements for background investigations and security clearances, as required by the Departmental Manual to ensure employees working on sensitive systems have the proper background and security clearances. A complete evaluation of position sensitivities **ASC**-wide and the assignment of sensitivity levels will be completed by April 1, 1999. However, the ASC has no control over when the background investigations on these employees will be completed. These investigations are performed by an outside contractor. We believe that the contractor can complete most of these investigations by October 1, 1999. The responsible official is the Chief, Applications Management Office.

Position sensitivity evaluations for the ADP Services Division have been completed and the results of several background investigations received. The **ASC** began position sensitivity evaluations in the FPPS Division in June of 1998 with background investigations to follow. Position sensitivity evaluations for the Financial Systems Division (FSD) and PAY/PERS Division will commence after management decisions are made regarding potential reorganizations impacting the positions in these divisions.

While the ASC can control the position sensitivity evaluation process, it cannot control the timeframes in which the background investigations and security clearances are completed. The audit recommendation states that the background investigations and security clearances should be completed before the individuals are assigned to the positions. Our understanding is that this criteria only applies to positions classified as "Sensitive" (of which ASC has had very few thus far). Therefore, our concurrence is based on the understanding that employees currently occupying positions classified as "Non-Sensitive" may continue in those positions until such time as completed background investigations either confirm or rebut the appropriateness of their placement in these jobs.

B. Operating Efficiencies

Condition: At the Service Center, each division controlled the process of moving changed

software from the test to the production environment, different software tools were used to control the movement of the changed software, and internal and external

clients controlled their mainframe computer production scheduling.

Criteria: Office of Management and Budget Circular A- 130 states that management should

oversee its processes to maximize return on investment and minimize financial and operational risk. Further, the Circular requires that financial management systems conform to the requirements of Office of Management and Budget Circular A-127, "Financial Management Systems." Circular A- 127 requires that agency financial

management systems process financial events effectively and efficiently.

Cause: Service Center management did not ensure that its processes were operating

efficiently because of preferences of internal and external clients and because management had not developed and implemented consistent standards for

controlling operational processes.

Effect: There was an increased risk that changed **software** would negatively impact the

mainframe computer operating system; costs of maintaining different software tools would increase Service Center operating costs, which would be passed onto clients; and **mainframe** computer usage could be reduced. Additionally, without centralized control of production scheduling, there was an increased risk that critical processing

jobs would not receive the required priority.

Recommendation:

We recommend that the Director, Administrative Service Center, in coordination with the Service Center's internal and external clients, evaluate the feasibility of centralizing the process of moving changed software from the test environment to the production environment, using standardized software tools to control the software change process, and centralizing mainframe computer production scheduling.

Response

Concur. The ASC will in coordination with internal and external clients perform an evaluation of the feasibility of centralized software change management. The feasibility analysis will include evaluating the viability of a standard software change management tool and make recommendations to management by October 1, 1999. In addition to evaluating centralized software change management, the ASC will also evaluate the feasibility of centralized computer production scheduling. Should the feasibility evaluation indicate that centralized change management and production scheduling is cost beneficial,

additional implementation time beyond the October 1, 1999, date will be necessary. The responsible official is the **Chief**, Applications Management Office.

There are several issues which this feasibility evaluation will need to consider. Due to the variety of customers ASC serves, centralized software change management will require technical expertise in a variety of different customer practices and utilities. Software change management is no longer simply a Common Business Oriented Language (COBOL) exercise. Without even considering the software change management tools our customers are using, there are multiple change management software tools even within the ASC. ChangeMan is the selected ASC change management software product that controls day-to-day changes on the IBM computer. This product is in various phases of implementation throughout the ASC. However, ChangeMan will not work within the COM-PLETE/Natural environment which FPPS uses. The PAC change management software tool was selected for this environment, due to the uniqueness of the Natural language. Since the intent of this recommendation appears to address the overall efficiency of mainframe computer operations, the intent of the feasibility evaluation will address this same concern as well.

SOFTWARE CHANGE MANAGEMENT

C. Application Software Change Management Controls

Condition: Software changes made to the FPPS during the latter stages of development and the early stages of implementation were not approved, reviewed, or evaluated adequately before changed **software** was installed for use in production; documentation was not adequate to monitor changes made to the software; and available library control software' was not implemented to ensure consistency and completeness throughout the FPPS application.

Criteria:

Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," provides guidelines for managing software maintenance. Publication 106 states that all software changes should be carefully evaluated and formally reviewed prior to installing the changed software. The publication further states, "In order to monitor maintenance effectively, all activities must be documented. ... The key to successful documentation is that not only must the necessary information be recorded, it must be easily and quickly retrievable by the maintainer." In addition, FPPS Division policies and procedures require that all changes to the FPPS application be thoroughly documented, be accepted by all involved parties, and pass a quality assurance review.

Cause:

FPPS Division management did not ensure that Division personnel followed software change management practices for making **software** changes to the FPPS application because of the time constraints to implement FPPS and because FPPS was encountering problems and was considered by Division personnel to be unstable. In addition, we found that FPPS Division management did not hold its personnel accountable for complying with Division policies and procedures when they made changes to the FPPS application. Further, FPPS Division management said that they did not implement the available library control software, which would ensure adequate documentation of the FPPS application, because at that time, the vendor library control software was not working correctly.

Effect:

There was an increased risk that the changes made to the FPPS application would not perform according to specifications, which could adversely affect user satisfaction and could adversely impact other applications interfacing with the FPPS application or the mainframe operating system.

Recommendations:

We recommend that the Director, Administrative Service Center:

^{&#}x27;Library control software is a system for keeping track of changes to and versions of software programs, documenting components to build executable programs, and preventing unauthorized access to program files.

1. Require that software changes be adequately reviewed and approved before the changes are implemented.

Response

Complied. Currently, FPPS Standard Operating Procedures (SOP) require that any software changes complete the following steps:

- Be approved by FPPS management before programming begins.
- Be migrated to a dedicated test environment upon completion with an explanation of the change(s) made.
- Be independently tested and approved for production by FPPS Functional Analysts and have the test results and documentation reviewed and approved by an FPPS Functional Lead.
- Be independently migrated to production by the FPPS Database Administrative staff along with any database changes required.

This **SOP** is enforced by FPPS Management.

Implement procedures to ensure that all software changes to the FPPS application are properly documented.

Response

Complied. The FPPS SOP requires that any software changes be fully documented on the change request form or problem report form. It also requires that any change (s) made be fully documented on the migration request forms and that a responsible person's signature be provided at each step along the way. Upon migration to production, all paperwork is filed for easy retrieval.

This SOP is enforced by FPPS Management.

3. Implement the available library control software when corrected to ensure adequate documentation of the FPPS application.

Response

Concur. The available library control software is in the process of being implemented for testing. Once it is to the stage that it will meet all our migration needs and is fully tested,

it will be implemented. The target date to debug, test, and render a "go or no-go" decision on implementation of available library control software is July 1, 1999. The responsible official is the Chief, Applications Management Office.

The FPPS SOP does provide adequate documentation and an organized systematic migration approach which also provides separation of duties. This SOP can also be used for emergency change reports which are a fact of life for any new system. One of the

reasons the library control software is not used is that it does not provide emergency change flexibility as our current SOP does. As FPPS completes the transition **from** a development mode to a maintenance mode, the computer operating environment will almost certainly change substantially. It will take time to determine how interrelated conditions will develop so **as** to determine specifically what corrections are needed to make the library control software operational.

SOFTWARE CHANGE MANAGEMENT

D. Operating System Software Change Management

Condition: Change controls over the mainframe computer operating system software were not adequate. The ADP Services Division change control procedures did not address adequate separation of duties between the development, test, and installation functions. Thus, one individual could perform all of these critical functions. In addition, the change control procedures did not ensure that all changes were properly approved by Division management. While the change management procedures required approval of all software changes, changes were made without documented evidence of approval.

Criteria:

Appendix III of Office of Management and Budget Circular A- 130 states that one of the minimum controls required in a general support system is personnel controls. One such control is separation of duties, which is "the practice of dividing the steps in a critical function among different individuals." Also, Federal Information Processing Standards Publication 106 states that "to be effective, the policy should be consistently applied and must be supported and promulgated by upper management to the extent that it establishes an organizational commitment to software maintenance. " In addition, Publication 106 states that "prior to installation, each change (correction, update, or enhancement) to a system should be formally reviewed." Finally, Division system change request procedures require that all change requests be approved by the appropriate branch chief

Cause:

ADP Services Division management did not ensure that appropriate separation of duties existed in developing and testing mainframe operating system software and parameter changes and in moving operating system software and parameter changes into the production environment, although the number of employees within the Division may allow for a separation of these duties. Additionally, Division management had not implemented controls to ensure that the process of making system software changes was in compliance with its documented procedures. Further, management had not implemented procedures to require periodic reviews of critical datasets and system parameters to identify inappropriate changes to the mainframe operating system environment. Although Division management had implemented a change control software tool that provided a systematic and automated means of controlling the movement of software changes, all the capabilities of the software tool were not implemented because of other Division priorities.

Effect:

There was an increased risk that unauthorized, untested, and undocumented changes could be made to the mainframe computer operating system **software** and parameters, which would affect system processing and data integrity, and that these changes would not be detected or detected in a timely manner.

Recommendations:

We recommend that the Director, Administrative Service Center:

- 1. Evaluate current ADP Services Division procedures and determine the feasibility of implementing controls in the change management process over operating system **software** to ensure that adequate separation of duties is addressed and complied with.
- 2. Develop procedures and implement controls to ensure that changes to the operating system parameters are identified, approved by ADP Services Division management, and documented.
 - 3. Develop procedures requiring periodic reviews of critical datasets and system parameters.
- **4.** Evaluate implementing available capabilities in the current change control **software** tool to more effectively control changes to the operating system software.

Response

Concur. The ASC will implement the recommended actions by July 1, 1999. The responsible official is the **Chief**, ADP Services Division.

MAINFRAME COMPUTER OPERATING SYSTEM SOFTWARE

E. System Audit Tools

Condition: Service Center management did not use available mainframe computer operating system audit tools that would improve integrity over system processing and data and that would detect inappropriate actions by authorized users. Specifically:

- Operating system integrity verification and audit software was not used. Such software could assist data center and installation security management in identifying and controlling the mainframe computer operating system's security exposures that may result from system setting options; from installing "back doors" to the operating system; and from introducing viruses and Trojan horses, which can destroy production dependability and circumvent existing security measures.
- Computer operators and system programmers had the capability to change the system initialization process and thus affect system processing. System options that would log the results in the SYSLOG² of actions taken by the computer operators and system programmers affecting mainframe operating system configuration were not implemented. Therefore, an audit trail of the system initialization process and changes to the operating system configuration could not be produced for periodic review. Based on recommendations made by our audit staff during the review, Service Center management implemented the logging capabilities within the system; however, procedures had not been developed and implemented to require periodic reviews of the logs.
- Periodic reviews of critical System Management Facility (SMF)³ logs to identify unauthorized changes to data by authorized users and critical events affecting system processing were not performed. For example, reviews were not performed of record type 7, which records when the system audit trail is lost, and record type 90, which records events such as SET TIME, SET DATE, and SET SMF, all of which affect system processing and audit trails.

Criteria:

Appendix III of Office of Management and Budget Circular A-130 requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, the Circular states that individual accountability is one of the personnel controls required in a general support system. The Circular further states that an example of one of the controls to ensure individual accountability includes reviewing or looking at

²SYSLOG is an audit trail that logs the results of actions taken by computer operators and system programmers during system initialization.

³The System Management Facility (SMF) logs record all system activity and serve as an audit trail of system activity, including identifying users who performed the activity.

patterns of users' behavior, which requires periodic reviews of the audit trails. Also, the National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" states that audit trails are "technical mechanisms" to achieve individual accountability.

Cause:

Service Center management did not acquire operating system integrity and verification software, did not encourage the use of available system audit trails to detect and identify inappropriate actions affecting the system processing and data integrity, and did not establish procedures requiring periodic reviews of available system logs. Instead, Service Center management relied on its **staff to** make appropriate changes to the system initialization process and on authorized users to make only appropriate changes.

Effect:

As a result, there was an increased risk that mainframe computer operating system security exposures would not be identified. Additionally, without periodic reviews of the system audit trails, there was an increased risk that processing problems or unauthorized activities would not be detected or detected timely and that the responsible individuals would not be held accountable for the inappropriate actions.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate acquiring system verification and auditing software.

Response

The ASC will develop functional requirements and identify additional resources necessary to manage and conduct evaluation of existing verification and auditing products to determine cost and capability. Should a software product be found which complies with our requirements, it will be implemented by January 1, 1999. The responsible official is the Chief, ADP Services Division.

2. Develop and implement procedures to ensure that periodic reviews are performed of the SYSLOG and critical SMF logs to identify unauthorized or inappropriate activities and that unauthorized or inappropriate activities are reported to Service Center management.

Response

Concur. The ASC will develop and implement procedures for reviewing SYSLOG and critical **SMF** logs by July 1, 1999. The responsible official is the Chief, ADP Services Division.

MAINFRAME COMPUTER OPERATING SYSTEM SOFTWARE

F. Mainframe Operating System Options

Condition: ADP Services Division management did not implement mainframe operating system options that would strengthen controls over computer programs which access sensitive operating system functions. We found 13 libraries that were able to run in the "Authorized Program Facility (APF)-authorized" state, even though the libraries were not required to run in the APF. By running in the APF-authorized state, these libraries may be considered part of the mainframe operating system and thus have access to all of the mainframe resources.

Criteria:

IBM's publication titled "OS/390 Initialization and Tuning Reference" states that "the parameter LNKAUTH specifies whether all libraries" in the LNKLST** member⁵ "are to be treated as Authorized Program Facility (APF)-authorized when accessed as part of the concatenation, or whether only those libraries that are named in the APF table are to be treated as APF-authorized." Additionally, the publication addresses managing system security and states that the "authorized program facility (APF) allows your installation to identify system or user programs that can use sensitive system functions. "

Cause:

Division Management implemented a default option (LNKLST) that allowed libraries within the LNKLST** member to run in the APF-authorized state. An alternative option (APFTAB) is provided which requires only those libraries that are named specifically in the APF table to be able to run in the APF-authorized state. The 13 libraries were automatically added to the **LNKLST**** member when the operating system was upgraded in July 1997. Because Division management did not review the members used to define APF-authorized libraries, these 13 libraries remained in the LNKLST** member. Further, because Division management implemented the LNKLST option, these 13 libraries were unnecessarily provided the ability to run in the APF-authorized state. Therefore, management did not have assurance that only approved libraries had access to sensitive operating system functions. Based on recommendations of our audit staff' during the review, the

⁴A library is a collection of programs or data files or a collection of functions (subroutines) that are linked into the main program when it is compiled. (The Computer Language Company, Inc., Computer Desktop Encyclopedia, Version 9.4, 4th Quarter, 1996.)

⁵Concatenation means to link together in a series or chain. (Webster's Ninth New Collegiate Dictionary, Merriam-Webster Inc., Springfield, Massachusetts, 1989, p. 27 1.)

LNKLST** member "defines the collection of program libraries to be searched, in sequence, for programs when no specific [library] has been supplied in the job stream." (Mark S. Hahn CONSUL Risk Management, Inc., A Guide to SYS1 PARMLIB, Monograph Series 4. The Information Systems Audit and Control Foundation, Inc., Rolling Meadows, Illinois, February 1996, p. 38.)

libraries were removed from the LNKLST** member. However, if the APFTAB option had been used, Division personnel would have been required to enter the 13 library names into the APF table, thus providing additional assurance that only approved libraries would run in the APF-authorized state.

Effect:

By implementing the LNKLST option rather than the APFTAB option, the risk increased for unauthorized libraries to run in an authorized state, thus bypassing operating system controls, and for system integrity to be lost.

Recommendations:

We recommend that the Director, Administrative Service Center:

1. Evaluate the feasibility of using the APFTAB option, thus providing additional assurance that only approved libraries would run in the APF-authorized state.

Response

Concur. The ASC will review the existing control methodology and determine if using the APFTAB option would provide enough additional safeguards to justify its implementation. The review will be completed and recommendations provided to management by July 1, 1998. The responsible official is the Chief, ADP Services Division.

2. Perform periodic reviews of all members used to define the APF-authorized libraries to ensure that only those required to run in the APF-authorized state are given this authority.

Response

Concur. The ASC will by October 1, 1998, develop procedures requiring periodic reviews of members used to define the APF-authorized libraries. The responsible official is the Chief, ADP Services Division.

STATUS OF CURRENT AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required	
C.l and C.2	Implemented.	No further action is required.	
A.1, A.2, B.1, C.3, D.1, D.2, D.3, D.4, E.1, E.2, F.1, and F.2	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.	

STATUS OF PRIOR AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.l, B.l, C.l, D.l, D.2, E.l, F.l, F.2, F.3, G.l, H.l, H.2, I.1, I.2, J.2, K.1, L.l, M.l, N.l, N.2, and 0.1	Implemented.	No further action is required.
D.3, G.2, and J.1	Resolved; not implemented.	No further response to the Office of Inspector General is required. The information regarding the status of these recommendations will be provided to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

Within the Continental United States

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 Washington, D. C . 20240

Our 24-hour Telephone HOTLINE 1-800-424-508 1 or (202) 208-5300

TDD for hearing impaired (202) 208-2420 or 1-800-354-0996

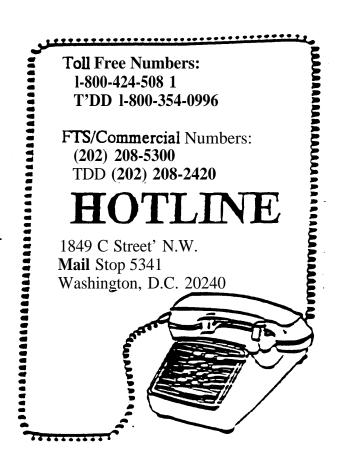
Outside the Continental United States

Caribbean Region

U. S. Department of the Interior Office of Inspector General Eastern Division - Investigations 4040 Fairfax Drive Suite 303 Arlington, Virginia 22201 (703) 235-922 1

North Pacific Region

U.S. Department of the Interior Office of Inspector General North Pacific Region 415 Chalan San Antonio Baltej Pavilion, Suite 306 Tamuning, Guam 96911 **(67** 1) **647-605** 1





U.S. Department of the Interior Office of Inspector General

EVALUATION REPORT

YEAR 2000 READINESS OF AUTOMATED INFORMATION SYSTEMS AT THE BUREAU OF RECLAMATION

> REPORT NO. 99-I-165 JANUARY 1999

BACKGROUND

The "Y2K problem" is the term used to describe the potential failure of information technology systems, applications, and hardware related to the change to the year 2000. Many computer systems that use two digits to keep track of the date will, on January 1, 2000, recognize "double zero" not as 2000 but as 1900. This could cause computer systems to stop running or to start generating erroneous data. The problem has been recognized as nationally significant by the President in Executive Order 13073, issued in February 1998. The Secretary of the Interior, in a December 1997 memorandum, stated that the Y2K problem was critical to the Department in meeting its mission and that resolution of the problem was one of his highest priorities. Further, Office of Management and Budget Memorandum 98-02, "Progress Reports on Fixing Year 2000 Difficulties," issued on January 20, 1998, requires all Federal executive branch agencies to ensure that Federal Government systems do not fail because of the change to the year 2000 and to have all systems, applications, and hardware renovated by September 1998, validated by January 1999, and implemented (that is, "fixes to all systems--both mission critical and non-mission critical") by March 1999. The Office of Management and Budget, in Memorandum 98-02, states that it is to provide "information to the Congress and the public as part of its [Office of Management and Budget's] quarterly summary reports on agency progress...[and] to report on the status of agency validation and contingency planning efforts and on progress in fixing, equipment that is date sensitive."

The Department has developed the "Department of the Interior Year 2000 Management Plan," which focuses on the resolution of the Y2K problem and provides an overall strategy for managing Departmental mission-critical systems and infrastructure. The Department has a multitiered approach to managing the Y2K problem that includes a top tier, which comprises the Secretary of the Interior; the Information Technology Steering Committee, which consists of the Chief of Staff and Assistant Secretaries; and the Chief Information Officer, who is responsible for the Department's Y2K issues. This tier, which represents senior-level Departmental managers, provides the Y2K project's direction and resources and ensures accurate reporting to external organizations, such as the Office of Management and Budget and the Congress. A DepartmentwideY2K project team, which reports to the Chief Information Officer and comprises representatives from each agency and the Office of the Secretary, is tasked with developing the Department's "Year 2000 Management Plan," refining inventory data on the Department's mission-critical and information technology portfolio systems,' and monitoring and reporting the progress of each conversion. In addition, a Y2K Embedded Microchip* Coordinators Team has been established to inventory

^{&#}x27;The portfolio is an inventory listing of 13 crosscutting or sensitive systems that are receiving attention at the Secretarial level.

^{&#}x27;Embedded microchips are "integrated circuits (miniature circuit boards)" that control "electrical devices," which include "elevators; heating, ventilation, and air conditioning (HVAC) systems; water and gas flow controllers: aircraft navigational systems; … medical equipment"; and office devices such as telephones, facsimile machines, pagers, and cellular telephones. (Department of the Interior's **Office** of Managing Risk and Public Safety "Year 2000 Embedded Microchip Hazards" [Web site])



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, DC. 20240

JAN - 8 1999

EVALUATION REPORT

Memorandum

Commissioner, Bureau of Reclamation To:

Director, Denver Administrative Service Center, Bureau of Reclamation

Robert J. Williams Potenty. cc account From:

Assistant Inspector General for Audits

Subject: Evaluation Report on Year 2000 Readiness of Automated Information Systems at

the Bureau of Reclamation (No. 99-I-165)

INTRODUCTION

This report presents the results of our evaluation of the year 2000 (Y2K) readiness of automated information systems at the Bureau of Reclamation and the Bureau's Denver Administrative Service Center. The objective of our review was to determine whether the Bureau inventoried its automated information systems and identified those systems that nere mission critical and were not Y2K compliant and whether the Bureau and the Service Center (1) developed auditable cost estimates for renovating systems to be Y2K compliant; (2) identified, by name, individuals responsible for ensuring that the Bureau is Y2K compliant; (3) ensured that responsible individuals' personnel performance evaluation plans included critical elements related to identifying and remedying Y2K problems; (4) developed a credible plan that included milestones and a critical path to ensure that the Bureau is Y2K compliant; and (5) developed a contingency plan that would address the failure of any part of the systems not being Y2K ready. This review was conducted at the request of the Department of the Interior's Chief Information Officer to assist the Information Officer in monitoring the progress of Departmental agencies in ensuring Y2K readiness, implementing Y2K compliant systems, and validating the accuracy of the information reported by the Departmental agencies to the Chief Information Officer.

and monitor embedded microchip technology Y2K problems. The team is led by the Office of Managing Risk and Public Safety and comprises representatives of the eight Departmental agencies, the Denver Administrative Service Center, and various Departmental offices.

The Department's May 15, 1998, "Progress Report," which was submitted to the Office of Management and Budget, reported that the Department had 91 mission-critical systems, of which the Bureau of Reclamation had 16 systems (see Appendix 1). In addition, the Federal Personnel Payroll System (FPPS), which was developed and maintained by the Service Center, is 1 of the Office of the Secretary's mission-critical systems and is 1 of the Department's 13 information technology portfolio systems. To address the Y2K problems, the Bureau established a Y2K project management structure. The structure included multiple "Coordination Teams," which were headed by an executive Y2K manager who is the Director of the Management Services Office, and the teams included the Reclamation Information Resources Management Coordinator, the Manager of the Policy and Program Management Group, the Bureau's IT (Information Technology) Security Manager, and Y2K coordinators at Bureau program and regional offices. The Service Center also established a Y2K project management structure that includes a Y2K executive, a Y2K program manager, a Y2K coordinator, and three Y2K program element leaders.

SCOPE OF EVALUATION

To accomplish our objective, we reviewed the documentation available that supported the Bureau's information submitted to the Department's Chief Information Officer for the May 1998 "Progress Report" and the documentation available that supported the information submitted by the Service Center to the Office of the Secretary. We performed our evaluation during April through July 1998 at the Reclamation Service Center's Management Services Office and the Denver Administrative Service Center, located in Denver, Colorado, and the Bureau's Eastern Colorado Area Office, located in Loveland. Colorado. We interviewed personnel responsible for project coordination to identify the Bureau's and the Service Center's Y2K plans and progress. We also interviewed personnel involved in various aspects of the Y2K project, including coordination. compliance identification, software remediation, and project management.

The evaluation was conducted in accordance with the "Quality Standards for Inspections," issued by the President's Council on Integrity and Efficiency, and included such tests and inspection procedures considered necessary to accomplish the objective. Our conclusions on the status of the progress made by the Bureau in addressing and remediating Y2K problems were based on reviews of documentation maintained by the Management Services Office and discussions with the Y2K coordinators throughout the Bureau and with individuals performing remediation or replacement of noncompliant applications or hardware. Also, our conclusions on the status of the progress made by the Denver Administrative Service Center were based on reviews of documentation and discussions with the Y2K program manager, the Y2K coordinator, the program element leaders, and individuals performing remediation or replacement of noncompliant applications or hardware. As specifically agreed to in our discussions with the Department's Chief

Information Officer, we did not validate or certify that the Bureau's or the Service Center's systems were Y2K compliant.

RESULTS OF EVALUATION

Regarding the six areas that the Chief Information Officer requested us to evaluate, we found that the Bureau had completed actions for two areas, had partially completed actions for three areas, and had not completed action for one area. Specifically, the Bureau had designated responsible officials and had inventoried its automated information systems, but the Department's Office of Information Resources Management agreed that the Bureau had to report only 16 of its 48 noncompliant mission-critical systems. Additionally, the Bureau had not included critical elements related to identifying and remedying Y2K problems in all responsible individuals' personnel performance evaluation plans; had not included all systems in its master plan, which had completion dates that were inaccurate; and had contingency plans that may not be adequate. For the remaining area, the Bureau had not developed auditable cost estimates. Because actions have not been completed for all areas, we believe that there is a risk that the Bureau may not meet the Office of Management and Budget's target date of March 1999 for having compliantY2K systems implemented.

Additionally, of the five areas that the Chief Information Officer had requested us to review, we found that the Denver Administrative Service Center had completed actions for three areas, had not completed actions for one area, and had determined that one area was not applicable. Specifically, the Service Center had developed a credible plan, including milestones; had designated responsible individuals; and had updated the annual personnel performance evaluation plans. However, the Center had not completed action on developing a contingency plan but had determined that the development of auditable cost estimates was not applicable to FPPS. As a result of the progress being made by Service Center Y2K project management, we believe that the Service Center will meet the Office of Management and Budget's target date of March 1999 for having compliant Y2K systems implemented for FPPS if the Y2K project proceeds as scheduled. If delays are encountered, development of contingency plans may be necessary.

The specific actions taken by the Bureau of Reclamation and the Service Center related to each area and other issues affecting the Bureau's and the Service Center's Y2K progress are discussed in the paragraphs that follow.

Automated Information Systems Inventory

Although the Bureau had performed an inventory of all of its automated information systems except for international project offices and identified 48 mission-critical systems. the Bureau's May 1998 "Quarterly Report" to the Department's Chief Information Officer showed only 16 noncompliant mission-critical systems. We found that the Bureau was reporting only 16 systems as mission critical because its Y2K project management did not use the Department's criterion for reporting mission-critical systems, which states that "those systems that when their capabilities are degraded, the organization realizes a resulting loss

of a core capability or life or property are threatened." Although Bureau Y2K project management did not use the Department's criterion for reporting, the Bureau received approval from the Department's Office of Information Resources Management to report only those systems that were to be repaired because of the large number of mission-critical systems that would otherwise have to be reported and managed. Therefore, Bureau Y2K project management said that it tracked and reported only systems that met all of the following Bureau criteria: (1) were mission critical, (2) were not Y2K compliant, (3) were date dependent, and (4) were being redeveloped or repaired. However, Office of Management and Budget Memorandum 98-02 requires that executive agencies report the "total number of mission-critical systems," as well as the "number compliant, number being replaced, number being repaired, and number being retired." As a result, the Bureau and Departmental Y2K project management were not tracking the replacement of Bureau mission-critical systems, such as the Mid-Pacific Region's Sutron Database System and the Centralized Water and Power System Control system, that were not Y2K compliant and were not reporting these systems to the Office of Management and Budget. However, in its September 23, 1998, response (Appendix 2) to the draft report, the Bureau stated that it is providing "high-level, ongoing management attention to ensure that all mission-critical applications will be Y2K compliant in sufficient time prior to January 2000."

Additionally, Y2K project management had not initially ensured that systems which had been identified by Bureau regional personnel as Y2K compliant were Y2K compliant. However, Y2K project management stated in exit conferences that a process was in place as of July 1998 to ensure that systems which had been identified by Bureau regional personnel as Y2K compliant are Y2K compliant.

We also found that the Bureau's method of reporting mission-critical systems to the Department's Chief Information Officer did not focus on the Bureau's mission and ability to perform its core capabilities and that each region was allowed to define its mission-critical systems. Therefore, the reporting of mission-critical systems was not consistent within the Bureau. For example, the Bureau tracked and reported the Upper Colorado Region's Colorado River Storage Project (CRSP) and the Great Plains Region's Wyoming Area Office Supervisory Control and Data Acquisition(SCADA)³ systems as mission critical. However, there are SCADA systems in the other regions, such as the Lower Colorado and the Mid-Pacific, that were identified as mission critical and not Y2K compliant at the time the inventory was completed but were not reported. By not ensuring that all mission-critical systems which support core capabilities are Y2K compliant before the year 2000, the risk is increased that some of the Bureau's systems may fail and that the Bureau may not be able to deliver water and hydroelectric power to its customers without incurring significant personnel costs.

The Department's Chief Information Officer requested that we determine the progress of the Bureau and the Service Center in addressing embedded microchips in information systems

³SCADA systems are systems that interface within selected water projects and are used by the Bureau to monitor and control water flow and hydroelectric power.

and facilities. We found that the Bureau and the Service Center, at the time of our review, had begun to inventory embedded microchips in information systems and facilities.

Auditable Cost Estimates

Of the 16 mission-critical systems reported to the Department's Chief Information Officer, documentation was maintained for 2 systems: the Technical Service Center's Data Acquisition and Management System (DAMS) and the Upper Colorado Region's CRSP SCADA system. We found that the cost estimate of \$9,000 for DAMS was auditable and that the revised estimate of \$285,300 for the Upper Colorado Region's CRSP SCADA system also was auditable.

Although cost estimates reported for the remaining 14 mission-critical systems were not auditable, we attempted to determine whether the methodologies used by Bureau personnel to develop the cost estimates were reasonable. Based on information from regional personnel responsible for developing the cost estimates, we found that the methodologies used varied. For example, cost estimates for the Modsim, the PNOPER, and the Hydromet PN1 systems in the Pacific Northwest Region were initially based on total lines of source code⁴ multiplied by \$1 SO. However, personnel in the Region said that because they believed the results were too high, they lowered the amounts for reporting purposes based on "best estimates." In addition, the EM340 terminal emulator in the Pacific Northwest Region was renovated to be Y2K compliant. However, we found that the renovation costs were \$35 rather than the \$5,000 reported. For the SCADA system in the Great Plains Region's Wyoming Area Office, personnel in the Region said that the amount was a "best estimate." For the Hydromet Support and the North Platte River Daily Water Accounting systems, which also are in the Great Plains Region, personnel in the Region said that the estimates were based on total lines of source code multiplied by \$ 1.50. Additionally, renovation of the Hydrological River Operations Study System (HYDROSS) at the Technical Service Center was estimated to cost \$5,680, which, according to the Y2K coordinator, was based on an estimated 2 weeks of effort (80 hours) multiplied by \$60 per hour. However, this formula would result in an estimate of \$4,800. In its response to the draft report, the Bureau stated that the costs were \$500 to renovate the EM340 terminal emulator and \$5,680 for the HYDROSS. However, because adequate documentation to support these costs was not provided and because the Bureau stated in its response that "in most instances there have been no means to track Y2K costs," we determined that the Bureau's reported estimated and actual costs were not auditable.

In its response to the draft report, the Bureau stated that the Office of Inspector General did not "expect consistent and auditable cost estimates at this point." However, we stated that we did not expect the Bureau to expend resources in correcting prior estimates but to ensure that future estimated and actual costs were supported and auditable.

⁴Lines of source code are statements and instructions used by the computer to execute the tasks of computer programs. (Computer Desktop Encyclopedia? Version 9.4, 4th quarter, 1996)

According to Service Center Y2K project management, the Service Center had not developed any cost estimates related to FPPS because the System was reported as compliant by design. Project management was aware that products and the mainframe operating system which were used to develop and operate FPPS were identified as not Y2K compliant. However, Service Center Y2K project management said that they considered the upgrades to these systems to be part of normal maintenance and not directly related to Y2K. Consequently, the cost estimates related to Y2K remediation were not applicable. However, if costs specifically related to remediating Y2K problems are identified, these costs should be reported to the Department's Chief Information Officer.

Designation of Responsible Individuals

We found that the Bureau had specifically designated, by name, the Y2K executive, the Bureau Y2K coordinator, and Y2K coordinators in each of the Bureau's regional offices in its "Year 2000 IT Comprehensive Plan." In addition, the Service Center had specifically named a Y2K executive, a Y2K program manager, a Y2K coordinator, and three Y2K program element leaders. Therefore, the Bureau and the Service Center had completed this requirement.

Annual Personnel Performance Evaluation Plans

The Secretary of the Interior's December 1997 memorandum required that "a critical performance element for identifying and remedying" the Y2K problem be included as part of each responsible official's annual performance plan. Responsible officials are defined in the memorandum as agency directors, agency Y2K executives, agency information resources management coordinators, safety officials, and all others as determined by the Y2K executives. We found that 5 of the 13 Bureau Y2K coordinators, the Bureau Information Resources Management Coordinator, and the Bureau Y2K executive had elements addressing Y2K objectives in their annual personnel performance evaluation plans. However, the remaining eight Bureau Y2K coordinators did not have such elements included in their annual personnel performance evaluation plans.

We found that all six members of the Denver Administrative Service Center'Y2K project team had elements addressing Y2K objectives in their annual personnel performance evaluation plans.

Plan for Milestones

We found that the Bureau had provided a reasonable basis for developing the master plan and critical paths for the systems reported to the Department as part of the progress reports. Specifically, the milestones established in the Bureau's master plan were developed by system owners or other responsible persons in each region who were knowledgeable of the systems, and the Bureau Y2K coordinator used a project management software tool to assist in developing the plan. However, as discussed in the section "Automated Information Systems Inventory" in this report, not all mission-critical systems had been included in the

master plan. In addition, although the initial milestones appear to be reasonable, some of the completion dates reported in the Bureau's progress report were inaccurate (see the section "Other Issues").

The Service Center had developed five action plans: (1) the "Year 2000 Conversion Project Action Plan," (2) the "DASC Telecommunications l-ear 2000 Compliance Plan," (3) the "DASC LAN/PC Systems Year 2000 Compliance Plan," (4) the "Y2K Embedded Chip Project Plan," and (5) the "FPPS Year 2000 Conversion Action Plan." All of these plans contain milestones and critical paths to addressY2K compliance for each system. Although these plans were internal Service Center documents that were not submitted to the Department's ChiefInformation Officer and dates were revised as necessary, we believe that the plans adequately identified milestones and critical areas. As of May 1998, these action plans had completion dates of March 1999 or earlier.

Contingency Plans

We found that the Bureau had contingency plans for 15 of the 16 reported mission-critical systems. The Bureau did not develop a contingency plan for the Pacific Northwest Region's EM340 system because Bureau management stated that this system was compliant and a contingency plan was not necessary. The contingency plans for the 15 remaining systems were not specifically related to Y2K but were existing plans for disasters such as floods or earthquakes at the project sites. If the systems fail on January 1, 2000, the Bureau's contingency plans are to perform the functions of these systems manually based upon the procedures defined in the disaster plans. The disaster recovery plans may not be adequate in the case of Y2K failures because of the possible length of time required to remediate the affected systems and the ready availability of people to repair lines of code or to perform the manual operations. The disaster plans n-e reviewedwere for specific projects or clusters of projects, such as for Hoover, Parker, and Davis Dams, and did not assess the impact on the Bureau for the loss of systems such as the SCADA. Further, the plans did not identify the number and experience level of personnel required to operate the Bureau's facilities manually and did not take into consideration the impact that embedded microchips in cellular phones, telephones, radios, and automobiles mayhave on the Bureau's ability to operate its facilities. For example, we found the following:

- Bureau management said that they believed "people will be available at the power plants to take over [operate the power plants manually]" if the Bureau's noncompliant SCADA systems, including hardware, software, and sensing devices, do not functionafter December 3 1, 1999. In the Department's May 1998 "Progress Report" to the Office of Management and Budget, the Bureau requested a waiver to the Dual Compensation Act' from the Office of Personnel Management to hire 10 power plant operators should the SCADA systems fail. In its response, the Bureau stated that two SCADA systems were not Y2K compliant and that "[m]ost operations managers do not expect a need for additional

⁵A waiver from the Act allows the Bureau to hire retired Federal employees without loss or reduction to the employees' entitlements.

help." Therefore, according to the Bureau. the request for 10 power plant operators was "Reclamation-wide in nature to cover unforseen contingencies." However, we continue to believe that if SCADA systems fail and the additional people required to operate water project gates and power plants manually are not readily available, the Bureau may not have control over water flow and its power plants.

- The North Platte River Daily Water Accounting system automates the daily accounting for stream flows, reservoir conditions, and ownership in the North Platte River Basin in Wyoming. We found that if the system fails, the Wyoming Area Office will be prevented from performing the daily accounting of the North Platte River Basin. Wyoming Area Office officials stated that the Bureau has a legal requirement to supply information generated by the system.

In its response to the draft report, the Bureau stated that although the Continuity of Operations Plans did not address the failure of "cellular phones, telephones, radios, and automobiles," the Bureau "cannot be held responsible for global and common possibilities outside our scope or ability to control." However, the Bureau stated that it is developing a contingency and management guide for power and water facilities. We believe that when contingency plans are completed, the Bureauwill be better able to ensure that its water and power facilities will operate beyond the year 2000.

The Denver Administrative Service Center had not developed contingency plans related to Y2K for the mainframe systems because: according to Service Center Y2K project management, the systems were to be Y2K compliant by the fall of 1998. Service Center Y2K project management stated that if this target date was not met, a contingency plan would be developed.

Other Issues

We found other issues that affect the Bureau's and the Service Center's Y2K readiness efforts which should be addressed as follows:

• Data Exchange. The Department of the Interior and the Office of Management and Budget required that an inventory of all data exchanges with outside parties be completed by February 1, 1998, and that coordination with these parties to determine a transition plan occur by March 1, 1998. We found that the Bureau had not met the Office of Management and Budget's target date in that only 22 of the 33 Bureau field offices responded to the Bureau Y2K coordinator's request for data exchange information as of May 1998.

The Service Center had inventoried its data exchanges, including external and internal interfaces, and had contacted responsible parties for all but 5 of the 48 interfaces identified in the inventory that were in use. According to Service Center Y2K project management, two of the five interfaces will be retired before the year 2000, and the remaining three interfaces were determined to be the receivers' responsibility. However, documentation was not available to support that these parties were contacted by Service Center project management to confirm responsibilities.

- Independent Verification and Validation. According to Bureau management, the independent verification and validation testing of mission-critical systems being renovated was to be performed internally by Bureau staff because of the expertise needed to test the systems and the cost involved in having independent verification and validation performed by outside contractors. According to Sen-ice Center Y2K project management, the Service Center, at the time of our review, was evaluating the use of a contractor to assist in the independent verification and validation testing of FPPS for Y2K. However, we found that neither the Bureau nor the Service Center had developed independent verification and validation test plans or performed independent verification and validation testing of mission-critical systems as of May 1998.
- Compliance Reporting. The Bureau had reported to the Department's Chief Information Officer that the Wyoming Area Office's SCADA system was compliant as of December 1997 except for certification of the system. However, based on information from Great Plains Regional personnel responsible for the system, we found, at the time of our review, that the repaired system had not been implemented. In its response to the draft report, the Bureau stated that the system had been implemented.

The Service Center's mainframe computer, the computer that operates FPPS and the Department's Federal Financial System (FFS), was reported to be compliant as of July 1997. However, we found that the Service Center's version of the mainframe computer operating system was not Y2K compliant and would not be compliant unless more than 100 program temporary fixes were implemented or the system was upgraded to a newer version of the operating system. Service Center Y2K project management said that they planned to upgrade to the newer version of the operating system and to test the upgraded operating system for Y2K compliance by August 1998. In addition, the Service Center reported that FPPS was compliant by design. However, the software products used to develop and operate FPPS were not Y2K compliant (see the section "Auditable Cost Estimates"). These issues were not addressed in the Service Center's information submitted to the Department's Chief Information Officer for the May 1998 "Progress Report."

- Vendor Certifications. We found that to determine the Y2K compliance of vendor-supplied hardware andsoftware, Service Center Y2K project management relied on the vendors' written certifications. However, when the vendors' certifications could not be obtained, information contained in the vendors' Internet home pages was used. Although the Service Center had requested written certifications of Y2K compliance from its 25 mainframe software vendors, Service Center Y2K project management had received only letters certifying Y2K compliance for the software in use from 6 of the vendors. As of May 1998, the status of the requests made to the data communication vendors by the Service Center was as follows:
- Responses had not been received from vendors on about 4 percent of the Service Center's components.
- Responses had been received from vendors stating that these components were Y2K compliant on about 18 percent of the components.

- Service Center Y2K project management was still addressing the Y2K problems for 35 percent of its data communication components through planned software upgrades, date independence, and end of life for hardware and software components (no longer needed).
- Service Center Y2K project management relied on Internet site information for the remaining 43 percent of the Service Center's components to ensure Y2K compliance.

However, Service Center Y2K project management stated that all data communication software and hardware would be tested where possible.

- System Component Consolidation. The Bureau reported each component of the Pacific Northwest Region's Sutron Hydromet system as an individual mission-critical system. However, personnel in that region responsible for the system said that these components should not have been reported individually. If the components were combined into one mission-critical Hydromet system, the number of mission-critical systems reported for the Pacific Northwest Region would be 5 rather than 10.
- System Owners. In the Bureau's Y2K master plan, regional offices rather than personnel were identified as system owners. Although the Bureau's master plan identified a contact (by name) for each of the mission-critical systems reported, we believe that the designation of regional offices as system owners did not meet the intent of the General Accounting Office's "Year 2000 Computing Crisis: An Assessment Guide," which the Department required bureaus to follow for Y2K project management and for identifying system owners.
- The Federal Financial System. During our review, we found that Bureau Y2K project management as a customer and Service Center Y2K project management as a service provider were concerned that the FFS Y2K testing may not be completed as scheduled. FFS is used by six bureaus within the Department of the Interior and by other Federal agencies. FFS is being renovated under the Office of the Secretary, and acceptance testing is the responsibility of the U.S. Geological Survey's Washington Administrative Service Center. Further, the Geological Survey's mainframe computer, which is the computer where FFS acceptance testing is performed and where FFS operates for three bureaus, had the same operating system as the Denver Administrative Service Center's mainframe computer (which is not Y2K compliant and will not be compliant unless more than 100 program temporary fixes are implemented or the system is upgraded to a newer version of the operating system). Bureau and Service CenterY2K project management said that they are not certain that FFS can be fully tested at either the Denver or the Washington Administrative Service Center until the upgraded version of the mainframe operating system has been implemented at each Additionally, the originally scheduled completion date of June 1998 for implementation of the renovated FFS was not feasible because the upgrade to the operating system was not available for testing until July 1998, and the Bureau and the Denver Administrative Service Center expressed concerns that problems related to Y2K could be encountered during fiscal year 1999.

On July 30. 1998, we held an exit conference with Y2K project management of the Denver Administrative Service Center and on August 6, 1998. with project management of the Bureau of Reclamation and the Chief Information Officer. Service Center Y2K project management generally agreed with the conclusions contained in this report. However, Bureau Y2K project management expressed concerns regarding our conclusions on the Bureau's reporting of mission-critical systems and adequacy of contingency plans. The Bureau provided additional information in its response. Specifically, the Bureau generally concurred with the report and said that it "will continue to focus on Y2K project issues" and on meeting Departmental and Office of Management and Budget milestone dates. Although the Bureau disagreed with our conclusion regarding the adequacy of its contingency plans and stated that only one SCADA will not be Y2K compliant by January 2000, it cited actions being taken which should enable the Bureau to meet the required milestones for having Y2K compliant mission-critical systems except for the "Mid-Pacific's CVACS." Based on discussions with Bureau Y2K project management and on the response, we made changes to the report as appropriate, and we have not made any recommendations.

Since this report does not contain any recommendations, a response is not required.

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, the monetary impact of audit findings, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of personnel at the Bureau of Reclamation's Management Services Office and regional offices and the Denver Administrative Service Center in the conduct of our review

BUREAU OF RECLAMATION/DENVER ADMINISTRATIVE SERVICE CENTER MISSION-CRITICAL SYSTEMS INVENTORY'

System Name or Acronym	Description	Estimated Cost for Compliance
Great Plains (GP) Hydromet Support	Provides Hydromet data reporting and maintenance functions and supports the capture and upload of data into Hydromet from outside sources.	\$50,000
EM340	Digital 340 Terminal Emulation software for Hydromet interfaces.	5,000
Hydromet PN 1	Yakima Hydromet System. Collects and processes hydrologic and meteorologic data on a near-real-time basis.	30,000
Inhouse Hydromet	Hydromet data analysis tools. Program uses the information from Hydromet to retrieve, compute, and convert data. This allows users to format reports and use the data for analysis and display.	16,000
Sutron Hydromet	Hydromet data collection, translation, and storage.	75,000
North Platte River Daily Water Accounting (NPRDWA)	Automated daily accounting of stream flows, reservoir conditions, and ownership in the North Platte River Basin in Wyoming.	60,000
Wyoming Area Office Supervisory Control and Data Acquisition (SCADA WYAO)	Monitors and controls 14 power plants and 3 irrigation canals, and controls flows in 5 river systems.	3,000
Inhouse Agricultural and Meteorology Data (AGRIMET)	Data analysis and formatting.	22,500

^{*}Information is **from** the "Department of the Interior Year 2000 Management Plan." issued in February 1998, and the Bureau of Reclamation's "Y2K Software Application Report," dated February 1998.

System Name or		Estimated cost for
Acronym	Description	Compliance
Inhouse River Operations	Data analysis tools. Program uses the information from Hydromet to retrieve, compute, and convert data. This allows users to format reports and use the data for analysis and display.	37,500
Model Simulator (Modsim)	River System Operations Simulation. River modeling and simulation program.	20,000
Pacific Northwest Operations (PNOPER)	Real-time hydrologic and meteorologic data to support the Bureau's water resource management mission. Supported functional areas include flood control, hydrologic and structural monitoring related to dam safety, irrigation water supply, power generation, dam operations, and water supply.	15,000
Umatilla Planning Module	River System Operations Simulation. River modeling and simulation program.	20,500
Y akima Planning Model	River Operations Simulation. River modeling and simulation program.	20,000
Data Acquisition and Management System (DAMS)	Instrumentation database.	9,000
Hydrological River Operations Study System (HYDROSS)	Water rights and supply accounting model used in river basin planning studies.	5,680
Colorado River Storage Project Supervisory Control and Data Acquisition (CRSP SCADA)	Remotely controls generation and water bypass for 8 hydroelectric plants, with a total of 19 generating units.	<u>285,300</u> "
Total		<u>\$674.480</u>

^{**}This revised estimated cost is the amount reported by the Department of the Interior to the Office of Management and Budget as of May 1998 in the Department's "Quarterly Progress Report."



United States Department of the Interior

BUREAU OF RECLAMATION

Washington, D.C. 20240

SEP 23 1998

D-5010

MEMORANDUM

To: Office of Inspector General

Acting Assistant Inspector General for Audits

From: Eluid L. Martinez

Commissioner/

Subject: Comments on the Draft Evaluation Report on Year 2000 Readiness of Automated

Information Systems (Assignment No. A-IN-BOR-OOl-98R)

Attached are comments on the Draft Evaluation Report on Year 2000 Readiness of Automated Information Systems (Assignment No. A-IN-BOR-OOl-98R) at the Bureau of Reclamation. We appreciate the opportunity to review and comment on the draftreport

The report reflects a nontechnical review of Year 2000(Y2K) readiness within Reclamation and the status of the Y2K project in light of Office of Management and Budget and Department of the Interior required guidelines and the six criteria requested for evaluation by the Department's Chief Information Officer. Discussions between our staffs during the preliminarydraft review period resulted in many requested corrections which are reflected in the referenced draft. However, we believe several general comments in the report are unsupported opinions of Reclamation operations. Our response reflects only a few of the items of concern from the draft report. Reclamation will continue to focus on Y2K project issues and meet every deadline imposed by the Department and OME.

We appreciate the difficulty of reporting on such a complex subject. We hope you will find the attached comments to be of assistance, and we will be pleased to providefurther information or clarification on any of the comments provided.

Attachment

cc: Assistant Secretary - Water and Science, Attention: Carla Burzyk (w/attachment)

Bureau of Reclamation

Comments on OIG Draft Evaluation Report Year 2000 Readiness of Automated Information Systems

(Assistant No. A-IN-BOR-118 00R)

General Comments

Results of Evaluation

All known systems were reported in the comprehensive plan sent to the Department of the Interior (DOI) June 1, 1997. Estimated completion dates have proven accurate with less than 5 percent error. For many years Reclamation has had complex Continuity of Operations Plans for all of our facilities. The draft implied these Plans did not address all of the specific and widespread contingencies that could occur as a result of the Y2K problem even though each facility is prepared for any potential disaster, includingY2K calamities. Reclamation is currently in the process of developing a "Y2K Contingency Planning and Management Guide for Power and Water Facilities" which should cover any anticipated shortfalls.

Automated Information Systems Inventory

At the time of the inventory, no definition for mission-critical systems was available fronDOI. Reclamation used a combination of definitions from the Department of the Air ForceY2K's criteria with a semblance of the actual mission of our Bureau. Reclamation did initially report more mission-critical systems in an attempt to fully recognize all Y2K issues. However, as a result of discussions with, and as directed by the Office of Information Resources Management (OIRM), Reclamation reduced to 16 the number of mission-critical systems that were to be repaired. Based on this guidance, and as a result of guidance from OIRM, Reclamation did not report mission-critical applications that were not Y2K compliant and were scheduled to be retired or replaced.

Reclamation does, however, recognize the concern expressed by theOIG with respect to ensuring that all mission-critical applications are addressed. In fact, we are cognizant of the need to ensure that these applications will continue to function after January 1, 2000, and are providing high-level, ongoing management attention to ensure that all mission-critical applications will bY2K compliant in sufficient time prior to January 2000.

Contingency Planning

Reference was made that nowhere in the facilities Continuity of Operations Plans was any consideration made in the event that cellular phones, telephones, radios, and automobiles may fail due to Y2K noncompliance. Reclamation cannot be held responsible for global and common possibilities outside our scope or ability to control. However, it is the nature of our workforce to be at the work site or be readily available to transit to the work site at a moment's notice.

Auditable Cost Estimates

The OIG stated that it did not expect consistent and auditable cost estimates at this point but rather. Reclamation should keep track of Y2K expenses from this point forward.

1

Specific Comments

- 1. Page 2. leading paragraph, third sentence: Should read March 1, 1999. This is the artificially mandated due date for implementation of all Y2K software applications. All systems with the exception of the Mid-Pacific's CVACS will be Y2K compliant and implemented by March 1, 1999.
- 2. Page 6. paragraphs 1 and 2: Since no "special" funding was or is available for Y2K efforts, Y2K costs were and are still taken out of operations and project funds as they currently exist in each office. In most instances there have been no means to trackY2K costs.
- 3. Page 6. paragraph 2. sentence 5: The actual cost to upgrade the terminal emulator package in EM340 was \$500, and the actual cost to complete the HYDROSS application renovation, including testing and implementation, was \$5,680.
- Page 7. paragraph 2: We concur that not all Y2K involved personnel had Y2K performance elements in their annual performance plans, including appropriate Reclamation executives, Since then, further direction has been disseminated from the Commissioner's office to assure the Y2K mission-critical element has been or will soon be added to all Y2K responsible personnel.
- 5. Paee 8. paragraph 2 under "Contingency Plans": The actual number of noncompliant SCADA systems within Reclamation was two, compared to the numerous SCADA systems found throughout Reclamation. It is believed that ten powerplant operators would more than cover these two SCADA sites. Most operations managers do not expect a need for additional help, since most feel they are already adequately stat-fed for such an emergency. The original request was Reclamation-wide in nature to cover unforeseen contingencies that may be outside our control.
- 6. Page 9. Dararrauh 5: Reclamation had received no IV&V plan guidance from either DOI or OMB at the time of the audit. However, OMB instructions specifying third party tests and directions have been given to allY2K involved personnel and offices throughout Reclamation.
- 7. <u>Paee 9. paragraph 6. compliance reporting:</u> The Y2K compliant SCADA system has been implemented at the Wyoming AreaOffice and is still running. The system did, however. show non-fatal errors relating to the four-digit year just introduced. These have since been repaired.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL

Internet/E-Mail Address

www.oig.doi.gov

Within the Continental United States

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240 Our 24-hour Telephone HOTLINE 1-800-424-508 1 or (202) 208-5300

TDD for hearing impaired (202) 208-2420 or 1-800-354-0996

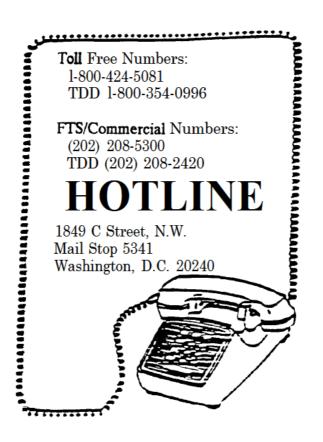
Outside the Continental United States

Caribbean Region

U.S. Department of the Interior Office of Inspector General Eastern Division - Investigations 4040 Fairfax Drive Suite 303 Arlington, Virginia 22203 (703) 235-9221

North Pacific Region

U.S. Department of the Interior Office of Inspector General North Pacific Region 415 Chalan San Antonio Baltej Pavilion, Suite 306 Tamuning, Guam 969 11 (67 1) 647-6060





U.S. Department of the Interior Office of Inspector General

EVALUATION REPORT

YEAR 2000 READINESS OF AUTOMATED INFORMATION SYSTEMS AT THE BUREAU OF LAND MANAGEMENT

> REPORT NO. 99-I-231 FEBRUARY 1999



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

FFB 1 2 1999

EVALUATION REPORT

Memorandum

To: Director, Bureau of Land Management

Robert J. Williams Poket & Walters
Assistant Inspector General for Audits From:

Evaluation Report on Year 2000 Readiness of Automated Information Systems Subject:

at the Bureau of Land Management (No. 99-I-23 1)

INTRODUCTION

This report presents the results of our evaluation of year 2000 (Y2K) readiness of automated information systems at the Bureau of Land Management. The objective of our review was to determine whether the Bureau (1) inventoried its automated information systems and identified those systems that were mission critical and were not Y2K compliant; (2) developed auditable cost estimates for renovating systems to be Y2K compliant; (3) identified, by name, individuals responsible for ensuring that the Bureau is Y2K compliant; (4) ensured that responsible individuals' personnel performance evaluation plans included critical elements related to identifying and remedying Y2K problems; (5) developed a credible plan that included milestones and a critical path to ensure that the Bureau is Y2K compliant; and (6) developed a contingency plan that would address the failure of any part of the systems not being Y2K ready. We also reviewed the Bureau's progress in inventorying automated information systems components, including computer software and hardware; telecommunications systems; facilities; and data exchanges between the Bureau and other Department of the Interior agencies or external entities for Y2K problems. This review was conducted at the request of the Department of the Interior's Chief Information Officer to assist the Information Officer in monitoring the progress of Departmental agencies in ensuring Y2K readiness, implementing Y2K compliant systems, and validating the accuracy of the information reported by the Departmental agencies to the Chief Information Officer.

BACKGROUND

The "Y2K problem" is the term used to describe the potential failure of information technology systems, applications, and hardware related to the change to the year 2000. Many computer systems that use two digits to keep track of the date will, on January 1, 2000, recognize "double zero" not as 2000 but as 1900. This could cause computer systems to stop running or to start generating erroneous data. The problem hasbeen recognized as nationally significant by the President in Executive Order 13073, issued in February 1998. The Secretary of the Interior, in a December 1997 memorandum, stated that the Y2K problem was critical to the Department in meeting its mission and that resolution of the problem was one of his highest priorities. Further, Office of Management and Budget Memorandum 98-02, "Progress Reports on Fixing Year 2000 Difficulties," issued on January 20, 1998, requires all Federal executive branch agencies to ensure that Federal Government systems do not fail because of the change to the year 2000 and to have all systems, applications, and hardware renovated by September 1998; validated by January 1999; and implemented (that is, "fixes to all systems--both mission critical and non-mission critical") by March 31, 1999. The Office of Management and Budget states in Memorandum 98-02 that it is to provide "information to the Congress and the public as part of its [Office of Management and Budget's quarterly summary reports on agency progress... [and] to report on the status of agency validation and contingency planning efforts and on the progress in fixing ... equipment that is date sensitive."

The Department has developed the "Department of the Interior Year 2000 Management Plan," which focuses on the resolution of the Y2K problem and provides an overall strategy for managing Departmental mission-critical systems and infrastructure. The Department has a multitiered approach to managing the Y2K problem that includes a top tier, which comprises the Secretary of the Interior; the Information Technology Steering Committee, which consists of the Chief of Staff and the Assistant Secretaries; and the Chief Information Officer, who is responsible for the Department's Y2K issues. This tier, which represents senior-level Departmental managers, provides the Y2K project's direction and resources and ensures accurate reporting to external organizations, such as the Office of Management and Budget and the Congress. A DepartmentwideY2K project team, which reports to the Chief Information Officer and comprises representatives from each agency and the Office of the Secretary, is tasked with developing the Department's Year2000 Management Plan, refining inventory data on the Department's mission-critical and information technology portfolio systems,' and monitoring and reporting on the progress of each conversion. In addition, a Y2K Embedded Microchip' Coordinators Team has been established to inventory and

-

^{&#}x27;The portfolio is an inventory listing of 13 crosscutting or sensitive systems that are receiving attention at the Secretarial level.

^{&#}x27;Embedded microchips are "integrated circuits (miniature circuit boards)" that control "electronic devices," which include "elevators, heating, ventilation and air conditioning (HVAC), water and gas flow controllers; aircraft navigational systems; and .. medical equipment" and office devices such as telephones, facsimile machines, pagers, and cellular telephones. (Department of the Interior's Office of Managing Risk and Public Safety "Year 2000 Embedded Microchip Hazards" [Web site])

monitor embedded microchip technology Y2K problems. The team is led by the Office of Managing Risk and Public Safety and comprises representatives of the eight Departmental agencies, the Denver Administrative Service Center, and various Departmental offices.

The Department's August 1998 "Quarterly Progress Report," which was submitted to the Office of Management and Budget, reported that the Department had 91 mission-critical systems, of which the Bureau had 13 systems (see Appendix 1). The Bureau has a project management team that comprises aY2K executive who is the Acting Assistant Director for Business and Fiscal Resources; a Y2K coordinator; Y2K managers at the Washington office, the 12 state offices, and the 6centers; and individual project managers for mission-critical systems, telecommunications, and embedded microchip technology efforts.

SCOPE OF EVALUATION

To accomplish our objective, we reviewed the documentation available that supported the Bureau's information submitted to the Department's Chief Information Officer for the August 1998 "Quarterly Progress Report." We performed our evaluation during June through September 1998 at the Bureau's Office of Information Resources Management Office, located in Washington, D.C., and the National Information Resources Management Center, located in Denver, Colorado. We interviewed personnel responsible for project coordination to identify the Bureau's plans and progress. We also interviewed, either in person, by telephone, or by electronic mail, personnel involved in various aspects of the Y2K project, including coordination, compliance identification, software remediation, and project management.

The evaluation was conducted in accordance with the "Quality Standards for Inspections," issued by the President's Council on Integrity and Efficiency, and included such tests and inspection procedures considered necessary to accomplish the objective. Our conclusions on the status of the progress made by the Bureau in addressing and remediating Y2K problems were based on reviews of documentation maintained by the Bureau's Information Resources Management, state, program, and center offices and on discussions with the various Y2K coordinators throughout the Bureau and with individuals performing remediation or replacement of noncompliant applications or hardware. As specifically agreed to in our discussions with the Department's Chief Information Officer, we did not validate or certify that the Bureau's infrastructure or systems wereY2K compliant.

RESULTS OF EVALUATION

Of the six areas that the Chief Information Officer requested us to evaluate, we concluded that the Bureau of Land Management, at the end of our fieldwork, had completed actions on

^{&#}x27;The 12 state offices are the Alaska, Arizona, California. Colorado, Eastern States, Idaho, Montana, New Mexico, Nevada, Oregon, Utah, and Wyoming State Offices. The six centers are the National Business Center, the National Human Resources Center, the National Information Resource Management Center. the National Interagency Fire Center, the National Applied Resource Sciences Center. and the National Training Center.

two areas but had not completed actions on four areas. Specifically, the Bureau had designated responsible individuals and developed contingency plans for its mission-critical systems. However, the Bureau had not reported all of its mission-critical systems to the Department's Chief Information Officer, developed auditable cost estimates, updated annual personnel performance evaluation plans, and developed credible plans that included milestones.

During our January 5, 1999, exit conference with Bureau of Land Management Y2K officials on the preliminary draft of this report, the officials provided updated documentation that would resolve the conditions identified in the preliminary draft report. Based on the documentation provided, we considered the actions on all six areas of the objective to be completed, and we have changed the report accordingly. The specific actions taken by the Bureau related to each area and other issues affecting the Bureau's progress are discussed in the paragraphs that follow.

Automated Information Systems Inventory

At the time of our review, the Bureau had not performed an inventory of all of its automated information systems. According to the Department's milestone dates, agencies were required to have mission-critical systems inventoried and systems that were not compliant identified by June 1997. Additionally, Memorandum 98-02 requires agencies to report on their total number of mission-critical systems. In the Department's August 1998 "Quarterly Progress Report," the Bureau reported that it had 13 mission-critical systems (see Appendix 1). Although the Bureau identified and reported 13 mission-critical systems, a complete inventory of its automated systems was not conducted and reported because the Bureau only inventoried and reported on its Bureauwide systems. We found that the Bureau had at least 11 additional systems which were critical to the Bureau's mission (see Appendix 2). For example, Oregon State Office Y2K project management identified eight mission-critical systems, of which three were related to the Bureau's mission of managing forests and wildlife habitat. Thus, there was a risk that all mission-critical systems had not been identified.

During the January 5, 1999, exit conference, Bureau Y2K officials provided documentation that resolved the identification of systems. While we believe that the mission-critical systems identified in Appendix 2 should have been reported to the Department as part of the Bureau's mission-critical systems, we also believe that the Bureau has adequately identified and implemented procedures which should ensure Y2K compliancy forall of the Bureau's systems. Therefore, the Bureau has completed this action.

The Department's Chief Information Officer requested that we determine the progress of the Bureau in addressing the Y2K problem regarding telecommunications and embedded microchips in information systems and facilities. We found, at the time of our review, that the Bureau's telecommunications coordinator had received inventory data from the 12 state offices and the 6 centers and that the Bureau's embedded microchip coordinator had received

complete inventory data from 6 of the 12 state offices and the 6 centers to construct a national database of mission-critical embedded microchip inventory data.

Auditable Cost Estimates

At the time of our review, we found that the cost estimates the Bureau reported to the Department's Chief Information Officer in the August 1998 "Quarterly Progress Report" were unauditable. The Bureau had not identified any costs for remedying the Y2K problem for seven of its mission-critical systems. Since these systems were to be repaired or redesigned, we believe that there should have been costs associated with these actions. The Bureau reported total estimated costs of \$250,000 to correctY2K problems in the six other mission-critical systems. However, the Bureau could not provide documentation to support its cost estimates for correcting the Y2K problems for these six systems. Therefore, the cost estimates were not supported or auditable.

In addition, the Bureau may have underestimated the costs to correct Y2K problems in embedded microchip technology. The Bureau reported costs of \$400,000 to correct embedded microchip technology Y2K problems to the Department's Chief Information Officer. However, we found that the estimated costs to correct embedded microchip technology in the Nevada State Office were estimated at more than \$540,000 and that, at the time of our review, only 6 of the 12 state offices and all 6 of the centers had completed inventories of embedded microchips.

During the January 5, 1999, exit conference, Bureau Y2K officials provided documentation that supported cost estimates for remedying the Bureau's mission-critical systems and correcting Y2K problems in its embedded microchip technology. Therefore, the Bureau has completed this action.

Designation of Responsible Individuals

We found that the Bureau had specifically designated, by name, the Y2K executive, the Bureau Y2K coordinator, Y2K managers in each of the Bureau's 12 state offices and 6 centers, and Y2K coordinators for embedded microchips and telecommunications. Therefore, the Bureau has completed this action.

Annual Personnel Performance Evaluation Plans

The Secretary of the Interior's December 1997 memorandum required that "a critical performance element for identifying and remedying" the Y2K problem be included as part of each responsible official's annual performance evaluation plan. Responsible officials are defined in the memorandum as agency directors, agency Y2K executives, agency information resources management coordinators, safety officials, and all others as determined by the Y2K executives. In addition, the Bureau Director issued Instruction Memorandum No. 98-127, "Year 2000 Critical Element for Employee Performance Appraisals," dated June 25, 1998, which required that a Y2K critical element be included in

the 1998 Employee Performance Plan and Results Reports for all responsible officials. These individuals included deputy directors and assistant directors, state directors, field and district office managers, center directors, state information resources management coordinators, official Y2K points-of-contact, and state safety officials. At the time of our review, we found that the Bureau Y2K coordinator and all responsible officials from the Idaho and Nevada State Offices and the National Interagency Fire Center, as well as some officials from the National Information Resources Management Center, had elements addressing Y2K objectives in their annual Employee Performance Plan and Results Reports. However, no documentation was provided to support that other Bureau Y2K responsible officials, such as the Y2K executive, the embedded microchip coordinator, the telecommunications coordinator, and the mission-critical systems coordinator, had such elements in their annual Employee Performance Plan and Results Reports.

During the January5, 1999, exit conference, BureauY2K officials provided documentation to support that the Bureau's Y2K executive, embedded microchip coordinator, telecommunications coordinator, and mission-critical systems coordinator had a critical performance element for identifying and remedying the Y2K problem in their annual performance evaluation plans. Therefore, the Bureau has completed this action.

Plan for Milestones

At the time of our review, we found that the Bureau had not developed credible plans which included milestones with critical paths for the 13 mission-critical systems reported as part of the Bureau's Y2K project. A Y2K Master Plan, dated January 1998, existed for 8 of the 13 mission-critical systems that included tasks, start and finish dates, and statuses, but the Plan did not contain procedures and milestones for each task to ensure that finish dates were met. In addition, the Bureau developed a draft Y2K Management Plan⁴ dated July 1998 that included milestones for completing various Y2K phases, such as assessment, renovation, validation, and implementation, for its mission-critical systems, embedded microchip technology, and telecommunications. However, the draft plan did not contain detailed steps for ensuring Y2K compliance for each of the Bureau's mission-critical systems. Further, the Bureau had not developed credible plans for the other 11 mission-critical systems (see section "Automated Information Systems Inventory").

During the January 5, 1999 exit conference, BureatY2K officials provided documentation to ensure that credible plans were developed for its mission-critical systems. In addition, Bureau officials provided us a copy of an updated Y2K Management Plan dated October 19, 1998, which included steps to ensure that its systems, hardware, software, telecommunications, embedded microchip technology, and data sharing arrangements would be Y2K compliant by the milestone date. Further, Y2K project management stated that certification documentation of Y2K compliancy for 11 of the Bureau's 13 mission-critical systems had been submitted to the Department's Chief Information Officer. The Bureau

⁴The draft Y2K Management Plan provides guidance to Bureau management and staff for ensuring Y2K readiness.

developed contingency plans for the other two mission-critical systems. Therefore, the Bureau has completed this action.

Contingency Plans

We found that the Bureau had a draft contingency plan dated July 1998 for the Automated Land and Mineral Record (ALMRS) and the Case Recordation and Mining Claims Recordation systems. The plan addressed contingencies in the event that ALMRS is not implemented by March 1999. The plan would require the Case Recordation and Mining Claims Recordation systems, which would be retired upon implementation of ALMRS, to continue operating. However, the hardware and the software to operate these systems need to be repaired to be Y2K compliant. The Bureau did not have contingency plans for any other mission-critical systems because the systems are scheduled to be compliant prior to March 1999. Therefore, the Bureau has completed this action.

Other Issues

We found other issues that affect the Bureau's readiness efforts which should be addressed as follows:

- Contract Language. Department of the Interior Acquisition Policy Release 1997-6, "Year 2000 Contract Specification," issued in April 1997, requires appropriate contract language to be included in all acquisitions that would pertain to Y2K compliance issues. However, the Bureau's contract for the ALMRS Modernization Project did not contain an amendment that included the appropriate contract language required by the policy release to ensure that the system would "either be year 2000 compliant as delivered or if noncompliant at that time be upgraded to be year 2000 compliant at no additional cost to the government." The Bureau initiated action to amend the ALMRS contract that was to have become effective beginning in fiscal year 1999.
- Independent Verification and Validation. According to the Bureau's Y2K project management, independent verification and validation testing of mission-critical and nonmission-critical systems are to be performed by an independent contractor. However, the costs associated with acquiring a contractor to perform the independent verification and the validation testing had not been estimated and reported at the time of our review (see section "Auditable Cost Estimates").
- Data Exchange. The Department of the Interior and the Office of Management and Budget required that an inventory of all data exchanges with outside parties be completed by February1, 1998, and that coordination with these parties to determine a transition plan occur by March1, 1998. We found that the Bureau had identified its data exchange partners and that the partners had been contacted by Y2K coordinators. The National Information Resources Management Center had identified five interfaces with systems external to the Bureau, and we verified that the inventory of data exchange partners was complete. The interfaces were with the Department's Minerals Management Service (three interfaces), the

Department's Office of Aircraft Services (one interface), and the Department of Agriculture's U.S. Forest Service (one interface). Bureau Y2K project management had contacted these entities and determined the appropriate actions to take to ensure that the exchanged data will process correctly after the year 2000.

Since this report does not contain any recommendations, a response is not required.

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, the monetary impact of audit findings, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of the Bureau of Land Management's Y2K coordinator, the Y2K coordinators at the state offices and centers, the mission-critical system coordinator, and other Bureau personnel in the conduct of this evaluation.

BUREAU OF LAND MANAGEMENT MISSION-CRITICAL SYSTEMS INVENTORY'

		Estimated
System Name or		Cost for
Acronym	Description	Compliance
Initial Attack	A system for tracking costs and	0
Management System	resources for wildlife suppression.	
Automated Land and Minerals Reporting System (ALMRS)	A system that tracks original land title information and mine leasing activities.	0
Case Recordation	A system that tracks land transfers, leases, and permitted uses of Federal lands. System will be replaced by ALMRS.	\$42,000
Mining Claims Recordation	A system that tracks unpatented mining claims, mill sites, and tunnels on Federal lands. System will be replaced by ALMRS.	0
Lease Management	A system that accounts for rents and fees associated with mineral leases and land use permits.	0
Aircraft Monitoring System	A system that tracks aircraft parts inventory and aircraft used by the Bureau of Land Management.	42,000
Cadastral Survey System	A system that tracks survey information related to public land surveys.	42,000
Inventory Data System	The system provides soil and vegetative data for analyzing and determining the best use of Federal lands.	40,000

^{*}Cost information is from the "Department of the Interior Year 2000 Management Plan," issued in February 1998. All other information is from the Bureau's Y2K Program Coordinator as of August 1998.

System Name or Acronym	Description	Estimated Cost for Compliance
Library Reference System	The system catalogs central library material.	0
Wildlife Inventory System	A system that tracks wildlife habitats, concentrating on endangered species.	42,000
Master Name System	The system provides a central repository of the Bureau's customer names and addresses.	0
Bond and Surety System	A system that tracks the status of companies authorized to issue bonds and sureties covering activities by operators on Federal lands.	0
Wild Horse and Burro System	A system that tracks the adoption and compliancy of adoptees of wild horses and burros.	<u>42.000</u>
Total		\$250,000

BUREAU OF LAND MANAGEMENT MISSION-CRITICAL SYSTEMS INVENTORY NOT BEING REPORTED TO THE DEPARTMENT

System Name and Acronym	Organization Identifying Systems as Mission Critical	
Automated Casefile Tracking System	Oregon State Office	
Micro*Storms (Forest Operations Unit Information)	Oregon State Office	
Procurement Information Network	Oregon State Office	
Road Appraisal System	Oregon State Office	
Spotted Owl Database	Oregon State Office	
Transportation Information Management System	Oregon State Office	
Timber Sale Information System	Oregon State Office	
Timber Volume and Value System	Oregon State Office	
Funds Accounting Control System (FACS)	Idaho State Office	
National Automated Cache System (NACS)	National Interagency Fire Center	
Automated Storage Conversion Distribution System (ASCADS)	National Interagency Fire Center	

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL

Internet/E-Mail Address

www.oig.doi.gov

Within the **Continental United States**

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240 Our 24-hour Telephone HOTLINE 1-800-424-508 1 or (202) 2085300

TDD for hearing impaired (202) 208-2420 or 1-800-354-0996

Outside the Continental United States

Caribbean Region

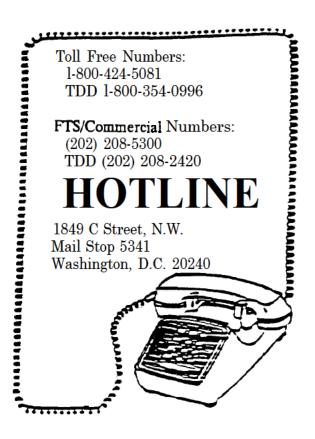
U.S. Department of the Interior Office of Inspector General Eastern Division - Investigations 4040 Fairfax Drive Suite 303 Arlington, Virginia 22203

(703) 2359221

North Pacific Region

U.S. Department of the Interior Office of Inspector General North Pacific Region 415 Chalan San Antonio Baltej Pavilion, Suite 306 Tarnuning, Guam 96911

(671) 647-6060





U.S. Department of the Interior Office of Inspector General

AUDIT REPORT

FOLLOWUP OF RECOMMENDATIONS FOR IMPROVING GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, BUREAU OF INDIAN AFFAIRS

REPORT NO. 99-I-454 JULY 1999



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington. D.C. 20240

JUL 2 6 1999

AUDIT REPORT

Memorandum

To: Assistant Secretary for Indian Affairs

Robert J. Williams Polet j. Williams
Assistant Inspector General for Audits From:

Audit Report on Followup of Recommendations for Improving General Controls Subject:

Over Automated Information Systems, Bureau of Indian Affairs (No. 99-1-654)

INTRODUCTION

This report presents the results of our audit of the implementation of recommendations contained in our April 1997 audit report titled "General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs" (No. 97-I-771) and our June 1998 audit report titled "Followup of General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs" (No. 98-I-483). The objective of our audit was to determine whether the Bureau of Indian Affairs had satisfactorily implemented the recommendations made in our prior audit reports and whether any new recommendations were warranted. This audit supports the Office of Inspector General's opinion on the financial statements of the Bureau and the Office of the Special Trustee for American Indians by evaluating the reliability of the general controls over computer-generated data that support the Bureau's and the Office of the Special Trustee's financial statements.

BACKGROUND

The Bureau's Office of Information Resources Management, through its Operations Service Center, both located in Albuquerque, New Mexico, is responsible for administering the general controls over the Bureau's and the Office of the Special Trustee's automated information systems. The Center provides computer services such as communications networks, software development, operations, and maintenance; systems recovery; and user support. The Center operates a Unisys server that is used to run the Office of the Special Trustee's applications, such as the Individual Indian Monies, and Bureau applications that

support Indian trust fund accounts. The Center also operated an IBM mainframe computer until December 1997, when the Bureau transferred its IBM operations and data processing functions to a host IBM mainframe computer owned by the U.S. Geological Survey's Enterprise Data Service Center, located in Reston, Virginia. The Geological Survey's IBM computer is used to run Bureau applications, such as the Land Records Information System and the National Irrigation Information Management System.

SCOPE OF AUDIT

Our audit included an evaluation of actions taken by Bureau management to implement the 12 recommendations contained in our April 1997 audit report and the 8 recommendations contained in our June 1998 audit report and a review of the general controls in place during fiscal year 1998. To accomplish our objective, we interviewed personnel at the Operations Service Center of the Bureau's Office of Information Resources Management, contractor personnel, and personnel at the Geological Survey's Enterprise Data Service Center. We reviewed the Bureau's policies and procedures as they related to the Bureau's computer operations, analyzed system security, and reviewed and tested implementation of the prior audit reports' recommendations. Because the highest priority of Center personnel at the time of our review was remedying applications for year 2000 (Y2K) compliancy, the availability of Center personnel was limited. Therefore, we performed limited testing of controls over the Unisys server.

The audit was conducted in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances to accomplish our audit objective.

As part of our audit, we evaluated the Bureau's general controls over its automated information systems that could adversely affect the data processing environment. The control weaknesses identified are discussed in the Results of Audit section. Because of inherent limitations in any system of internal controls, losses, noncompliance, or misstatements may occur and not be detected. We also caution that projecting our evaluations to future periods is subject to the risk that controls or the degree of compliance with the controls may diminish.

RESULTS OF AUDIT

We concluded that the general controls over the Bureau of Indian Affairs automated information systems were ineffective in the areas of its security program, access controls, software development and change controls, segregation of duties, and continuity of service. The Bureau continued to have ineffective general controls because Bureau management had not ensured that the recommendations contained in our April 1997 and June 1998 audit reports were implemented (see Appendices 1 and 2, respectively). Specifically, of the 20 recommendations from our prior audit reports, the Bureau had implemented 3 recommendations and had partially implemented 6 recommendations, but it had not

implemented the remaining **11** recommendations. Office of Management and Budget Circular A- 123, "Management Accountability and Control," states:

Resolution of Audit Findings and Other Deficiencies. Managers should promptly evaluate and determine proper actions in response to known deficiencies, reported audit and other findings, and related recommendations. Managers should complete, within established time frames, all actions that correct or otherwise resolve the appropriate matters brought to management's attention. ... Correcting deficiencies is an integral part of management accountability and must be considered a priority by the agency. [Managers are required to report in their annual integrity report to the President and the Congress any significant deficiencies and related risks.]

In addition, Circular A-123 states that deficiencies which are significant should be considered a "material weakness." It further states that deficiencies are significant when the management controls (1) do not provide assurance that assets are safeguarded against waste, loss, unauthorized use, or misappropriation and (2) are not adequate to protect the integrity of Federal programs or to ensure that resources are used consistent with the agency's mission; laws and regulations are followed; and reliable and timely information is obtained, maintained, reported, and used for decision making.

Additionally, publications of the Office of Management and Budget and the National Institute of Standards and Technology require Federal agencies to establish and implement management and internal controls to protect sensitive information in general support' and major application systems. Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," states:

Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Adequate security means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Since the recommendations from our prior audit reports have not been implemented, the Bureau is at risk of loss, misuse, modification of, or unauthorized access to the data in its automated information systems. Further, because the Bureau had not made significant

^{&#}x27;Office of Management and Budget Circular A- 130 defines a general support system or system to mean "an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications and people."

progress in correcting deficiencies in the general controls over its automated systems, we believe that the Bureau is not in compliance with the Federal Financial Management Improvement Act and should report these deficiencies to the Department as a material weakness in the Bureau's annual assurance statement on management controls, which is required by the Federal Managers' Financial Integrity Act.

The impact on the Bureau's general controls as a result of the Bureau's lack of implementation of the related recommendations is discussed in the sections that follow.

System Security Program

The Bureau did not have an effective system security program that included an information resource management strategic plan, periodic risk assessments, periodic assessments of the system security program's effectiveness, and personnel security policies and procedures to ensure that appropriate security clearances for personnel in sensitive or critical automated data processing (ADP) positions were obtained. We made nine recommendations relating to this weakness in the prior reports (Nos. A.1, A.2, A.3, and B.1 in our April 1997 report (see Appendix 1) and Nos. A.1, A.2, A.3, A.4, and A.5 in our June 1998 report (see Appendix 2)). During our current audit, we found that the Bureau had implemented one recommendation and had partially implemented two recommendations, but it had not implemented the remaining six recommendations. Therefore, the Bureau had little assurance that its information resources were used and managed effectively to accomplish its mission or that established controls could be relied on to protect mission-based sensitive computer systems and data.

Access Controls

Physical and logical access controls over the Bureau's automated information systems were ineffective. Specifically, the Bureau did not classify its resources to determine the level of security necessary, monitor visitor activities while at the Center, perform periodic reviews to ensure that users' access levels to the mainframe computers were appropriate, and change passwords to access the Unisys computer periodically. We made six recommendations relating to this weakness in the prior reports (Nos. C. 1, D.1, D.2, and E. I in our April 1997 report (see Appendix 1) and Nos. A.6 and A.7 in our June 1998 report (see Appendix 2)). During our current audit, we found that the Bureau had partially implemented two recommendations but had not implemented four recommendations. Therefore, the Bureau had little assurance that the most cost-effective access controls were in place to protect its computer resources; that the computer resources located in the Center's computer operations room, such as the mainframe computer, local area network (LAN) equipment, and daily backup tape libraries, were safeguarded from dust or fire hazards; that user access was assigned at the appropriate level; and that password controls were adequate.

Software Development and Change Controls

Software development and change controls were inadequate to ensure that the proper version of an application was used in production. For example, the programmers of the National Irrigation Information Management System and the Loan Management Accounting System not only programmed the application but also tested, authorized, and approved the movement of the modified programs from test or development into production. In addition, requests to change or modify the applications were not fully documented. We made one recommendation relating to this weakness in the prior report (No. G.l in our April 1997 report (see Appendix 1)). During our current audit, we found that the Bureau had not implemented this recommendation. Therefore, the Bureau had little assurance that only authorized programs and authorized modifications were implemented; that all programs and program modifications were properly authorized, tested, and approved; and that access to and distribution of programs were carefully controlled.

Segregation of Duties

Duties were inadequately segregated for the systems support functions in the areas of system design, applications programming, systems programming, quality assurance/testing, library management, change management, data control, data security, and data administration. We made one recommendation relating to this weakness in the prior report (No. H. 1 in our April 1997 report (see Appendix 1)). During our current audit, we found that the Bureau had partially implemented this recommendation because the IBM computer operations, such as system design and system programming, were transferred to the Geological Survey. However, the Bureau's separation of duties for system functions continued to be inadequate in the areas of applications programming, quality assurance/testing, library management, change management, data security, and data administration. Therefore, the Bureau had little assurance that programmers were making only authorized program changes; that computer programmers were independently writing, testing, and approving program changes; or that errors or illegal acts would be detected or detected timely.

Service Continuity

The Center did not have an effective means of recovering or of continuing computer operations in the event of system failure or disaster. Specifically, the Bureau's backup information, such as software applications and databases, was stored on-site in the Center's computer operations room rather than in an off-site storage facility. We made two recommendations relating to this weakness in the prior reports (No. J. 1 in our April 1997 report (see Appendix 1) and **No.** A.8 in our June 1998 report (see Appendix 2)). During our current review, we found that the Bureau had implemented one recommendation and had partially implemented the other recommendation. Therefore, there was no assurance that the Center would be able to recover or resume critical computer operations in the event a system failed or a disaster occurred.

We recommend that the Assistant Secretary for Indian Affairs report the Bureau's ineffective general controls over its automated information systems as a material weakness in the Bureau's annual assurance statement, which is required by the Federal Managers' Financial Integrity Act.

Bureau of Indian Affairs Response and Office of Inspector General Reply

In the June 3, 1999, response (Appendix 3) to the draft report from the Assistant Secretary for Indian Affairs, the Bureau concurred with the recommendation. Based on the response and subsequent discussions, we consider the recommendation resolved but not implemented. Accordingly, the recommendation will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (see Appendix 4).

Regarding our April 1997 report, the Bureau, in its June 1999 response, included a revised corrective action plan. Based on our current audit and the Bureau's response, we consider 2 recommendations (Nos. H. 1 and I. 1) resolved and implemented and 10 recommendations (Nos. A. 1, A.2, A.3, B. 1, C. 1, D. 1, D.2, E. 1, G.1, and J. 1) resolved but not implemented. Accordingly, the updated information on the prior recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget (see Appendix 5).

Regarding our June 1998 report, the Bureau, in its June 1999 response, included a revised corrective action plan. Based on our current audit and the Bureau's response, we consider three recommendations (Nos. A.l, A.3, and A.8) resolved and implemented and the remaining five recommendations (Nos. A.2, A.4, A.5, A.6, and A.7) resolved but not implemented. Accordingly, the updated information on the prior recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget (see Appendix 6).

Since the recommendation contained in this report is considered resolved, no further response to the Office of Inspector General is required (see Appendix 4).

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Bureau personnel in the conduct of our audit.

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR AUDIT REPORT "GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, OPERATIONS SERVICE CENTER, BUREAU OF INDIAN AFFAIRS" (NO. 97-I-771)

Recommendations

A. 1. The information technology security function is elevated organizationally to at least report directly to the Director, Office of Information Resources Management; is formally provided with authority to implement and enforce a Bureauwide

implement and enforce a Bureauwide system security program; and is provided staff to perform the required duties, such as providing computer security awareness training and performing periodic risk

assessments.

Status of Recommendations and Corrective Actions

Partially implemented. The Bureau of Indian Affairs stated that the Information Technology (IT) Security Manager had reported to the Director, Office of Information Resources Management, since October 1997 and that the position had Bureauwide authority for the information technology security program. The Bureau also stated that sufficient staff would be available to manage security requirements once the transfer to the host IBM computer at the U.S. Geological Survey had taken place. We found that the Security Manager reported to the Director, Office of Information Resources Management; however, we did not find that the Security Manager had acted on the authority to implement a Bureauwide security plan. Although authority is implied in the position description, the Bureau had not ensured that the Security Manager's authority was recognized by all Bureau personnel. In addition, the Security Manager is physically located at the Operations Service Center and has focused on Center security and user access to the IBM mainframe and Unisys server rather than on Bureauwide system security issues. We also found that additional staff had not been assigned to assist in providing security awareness training and performing risk assessments when the IBM operations

were transferred to the host computer at the Geological Survey.

A.2 A system security program is developed and documented which includes the information required by the Computer Security Act of 1987 and Office of Management and Budget Circular A-1 30, Appendix III, "Security of Federal Automated Information Resources," and policies and procedures are implemented to keep the system security program current.

Not implemented. The Bureau stated that it had entered into an agreement with the Geological Survey's Washington Administrative Service Center - West to develop, by July 31, 1998, a comprehensive security plan. The "Bureau of Indian Affairs Logical Security Internal Procedures Manual" was delivered to the Bureau during our site visit in September 1998. However, the plan was not Bureau specific but rather an overview of the Geological Survey's security for its IBM computer located in Reston, Virginia. Additionally, we found that policies and procedures were not developed and implemented to keep the system security program current.

A.3. The Bureau's security personnel perform risk assessments of the Bureau's automated information systems environment and, as appropriate, provide assurance that the necessary changes are implemented to manage the risks identified.

Not implemented. The Bureau stated that its information systems security staff would oversee this effort beginning in fiscal year 1999. However, we found that management had not developed a security program; therefore, plans had not been developed to begin risk assessments in fiscal year 1999.

Status of Recommendations and Corrective Actions

Recommendations

B. 1. Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel in sensitive or critical automated data processing (ADP) positions and for informing the security staff, in writing, whenever employees who are system users terminate their employment or are transferred.

Partially implemented. The Bureau stated that it had reorganized its position sensitivity program and that, as part of the effort, it had begun to review all sensitive positions. We found that personnel policies and procedures had not been developed or implemented to ensure that appropriate security clearances for personnel in sensitive or critical ADP positions were obtained or that security staff were notified in writing when employees terminated their employment or were transferred. However, during our site visit, the Security Manager was working with the Bureau's Central Office in reviewing the sensitivity levels of personnel assigned to the Operations Service Center. In addition, the Bureau stated that the Security Manager would ensure that the employee termination report was received and reconciled with system users. During our site visit, Bureau management had not agreed on how the termination report would be provided to the Security Manager.

Status of Recommendations and Corrective Actions

C.1. Develop and implement policies to classify the Bureau's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A-130. Appendix III.

Not implemented. The Bureau stated that risk assessments and classifications of its automated information systems environment would be performed beginning in fiscal year 1999 in accordance with its security program plan. According to the Bureau, assessments would be performed by teams consisting of personnel from the Bureau's Office of Information Resources Management and program offices. We found that policies which would ensure that computer resources were classified in accordance with Circular A- 130 had not been developed or implemented.

D. 1. Ensure that sufficient staff are provided to adequately monitor all visitor activities.

Not implemented. The Bureau stated that the recommendation had been implemented to the extent possible given the Bureau's available resources. The Bureau further stated that the organizational element receiving the visitors would monitor visitor activities. We found, during our site visit, that Center management did not consistently monitor visitors' activities.

Status of Recommendations and Corrective Actions

D.2. Ensure that funding is provided for adequate maintenance of the computer operations room, such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room.

Partially implemented. The Bureau stated that it had provided funds to the Center for full-time housekeeping and maintenance services for the computer room beginning in fiscal year 1998. We found that the Bureau had provided for daily housekeeping services and that the fireproducing equipment was no longer in use. Although housekeeping services were being performed and the fire-producing equipment identified in the prior report was no longer in use, the Center was using the computer operations room as a storage facility, which increased the risk of equipment failure and other fire hazards. For example, cardboard boxes of old records and old computer equipment were stored in the computer operations room.

E. 1. Ensure that policies are developed and implemented which match personnel tiles with system users periodically, that user identifications (IDs) are deleted from the system for users whose employment had been terminated, and that verification and approval are obtained from user supervisors and application owners or managers that the levels of access are appropriate.

Not implemented. The Bureau did not address this recommendation. We found that new or revised policies had not been developed which would match personnel tiles with system users periodically, delete user IDs from the system for users whose employment had been terminated, and ensure that verifications and approvals were obtained from users' supervisors and application owners that the users' levels of access were appropriate.

F. 1. Ensure that a higher priority is given to moving the applications that reside on the Unisys mainframe to the IBM mainframe.

Resolved. In the June 1998 audit report, we recognized that the recommendation was no longer applicable because the Bureau had determined that the Unisys applications could not be moved to the IBM mainframe.

Status of Recommendations and Corrective Actions

G.1. Ensure that policies and procedures are developed and implemented which clearly identify the individuals responsible and accountable for application development and changes.

H. 1. Ensure that staffing at the Center is evaluated and adjusted so that duties for critical system support functions are adequately segregated and fully utilized. Not implemented. The Bureau stated that the Applications Support Branch would develop the policies and procedures. However, we found that the Branch's highest priority was the Bureau's Y2K effort; thus, the policies and procedures had not been developed.

Implemented. The Bureau did not address this recommendation in its responses to our prior audit reports; however, for the IBM mainframe applications, the recommendation was resolved with the transfer of the Bureau's mainframe operations to the Geological Survey's host computer. We could not verify whether the critical system support functions for the Unisys server were adjusted during our fieldwork because Center personnel were involved with the Bureau's Y2K testing and were therefore not available. Based on the Bureau's June 3, 1999, response to the draft report, we consider the recommendation implemented because the Bureau stated that it is examining organizational changes and personnel assignments to ensure that duties are separated. The Bureau further stated that it will continue to monitor its progress in separating critical system support functions.

Status of Recommendations and Corrective Actions

Implemented. The Bureau transferred its

- I. 1. Ensure that access and activities of the Center's system programmers are controlled and monitored by security staff and that RACF controls are established to protect system resources.
- IBM computer operations to the Geological Survey's host computer. After the transfer, the Geological Survey established the appropriate RACF controls that would protect the system resources, which included denying the Bureau's system programmer access to the IBM computer's system controls.

J. 1. Ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility.

Partially implemented. The Bureau stated that it had a disaster recovery contract which fully tested and certified the Unisvshosted applications. However, although a contingency plan had not been developed, the Bureau had contracted for a backup site for the Unisys server in the event of a disaster and had tested the functionality of the backup site. The Geological Survey is responsible for contingency planning for the Bureau's IBM applications that reside on the Geological Survey's host computer. Additionally, although the Bureau had provided funding for off-site storage of its backup media, the Center had not used the site. The Bureau's backup media were stored on-site in the Center's computer operations room.

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR AUDIT REPORT "FOLLOWUP OF GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, OPERATIONS SERVICE CENTER, BUREAU OF INDIAN AFFAIRS" (NO. 98-I-483)

Recommendations

Status of Recommendations and Corrective Actions

A. 1. Establish as a high priority the use of the Geological Survey's host computer's operating, security, and automated job scheduling systems.

A.2. Develop and approve an Office of Information Resources Management strategic plan that provides direction to and defines the functions of the Operations Service Center.

Implemented. The Bureau of Indian Affairs transferred its IBM mainframe operations to the Geological Survey's host computer in December 1997. We reported this recommendation as implemented in our June 1998 audit report.

Not implemented. The Bureau stated that a strategic plan for the Office of Information Resources Management was being developed and finalized under a contract. The strategic plan was to have been completed by September 30, 1998. We found that the contract, dated March 9, 1998, was to support the Bureau's overall Information Resources Management strategic and tactical plans. However, contract performance was based on task orders, and at the time of our site visit, a task order had not been issued to develop a strategic plan.

Status of Recommendations and Corrective Actions

A.3. Hold the Information Technology (IT) Security Manager accountable for performing the position responsibilities.

Implemented. The Bureau stated that the IT Security Manager would be held accountable through the performance appraisal process. However, we found that the IT Security Manager had not been held accountable for not implementing a Bureauwide security program, providing security awareness training, or performing risk assessments. Additionally, the IT Security Manager performed the functions of a local area network (LAN) administrator, which was not part of the IT Security Manager's duties. Based on the Bureau's June 3, 1999, response to the draft report, we considered the recommendation implemented because the Bureau stated in its response that the IT Security Manager will be evaluated based on his performance standards and position description. The response further stated that the Division of Information Resources Management is in the process of "augmenting its IT security staff."

Status of Recommendations and Corrective Actions

A.4. Periodically perform an evaluation of the system security program's effectiveness and include any resultant corrective actions in future Bureau security plans.

Not implemented. The Bureau stated that it had entered into an agreement with the Washington Administrative Service Center - West to develop a comprehensive computer security plan. The plan's operating procedures and the management control reviews required by the Department of the Interior's Office of Information Resources Management would ensure that the plan would be reviewed periodically and updated. The plan was to have been developed by July 3 1, 1998. The Center received the "Bureau of Indian Affairs Logical Security Internal Procedures Manual" in September 1998. We found that the "Manual" was not Bureau specific but generally related to the Geological Survey and did not provide procedures for performing evaluations of the system security program. In addition, an evaluation of the system security program's effectiveness had not been performed in fiscal years 1996, 1997, or 1998.

AS. Redetermine, based on the Office of Information Resources Management's strategic plan, when the Bureau can begin performing risk assessments and classifying its resources. Also, personnel who will be responsible for the risk assessments and resource classifications should be identified.

Not implemented. The Bureau stated that risk assessments and classifications of its automated information systems environment would be performed beginning in fiscal year 1999 in accordance with its security program plan. However, the Bureau had not developed a security program; therefore, plans had not been developed to begin risk assessments in fiscal year 1999, and personnel responsible for the risk assessments and resource classifications had not been identified.

positions

A.6. Obtain security clearances for ADP personnel who are not assigned to the Center that are commensurate with their

A.7. Require Bureau staff to review and validate the appropriateness of users' levels of access to the Bureau's IBM applications. If the users' levels of access are not reviewed and validated by Bureau personnel, the Bureau should modify its agreement with the Geological Survey to include the requirements that access reviews and verifications should be performed for the IBM applications by the Geological Survey.

A.8. Remove all safety hazards from the computer operations room.

Status of Recommendations and Corrective Actions

Not implemented. The Bureau had begun to review and reassign security clearances for ADP personnel as a result of a Bureauwide initiative started in February 1998. During our site visit, the Security Manager was reviewing security clearances for Center personnel but had not begun to review clearances for personnel outside the Center.

Partially implemented. Under the direction of personnel of the Geological Survey's Enterprise Data Service Center, the Security Manager had begun to review the appropriateness of users' levels of access to the Bureau's IBM applications. Although the Bureau had begun negotiations with the Geological Survey to ensure that users' levels of access were reviewed jointly by the Bureau and the Geological Survey, the Bureau had not finalized the negotiations by signing the agreement.

Implemented. The Bureau stated that safety hazards had been removed. During our site visit, we found that the safety hazards had been removed.



United States Department of the Interior

OFFICE OF THE SECRETARY WASHINGTON, D.C. 20240

JUN 3 1999

Memorandum

To: Assistant Inspector General for Audits

From: Assistant Secretary - Indian Affaire Lucie Soul

Subject: Draft Audit Report on Follo wup of Recommendations for Improving General Controls

Over Automated Information Systems, Bureau of Indian Affairs (Assignment No. A-

IN-BIA-002-98-M)

The subject audit report addresses the Bureau of Indian Affairs' implementation of recommendations made by the Office of Inspector General (OIG) in April 1977, and June 1998, audit reports on the Operation Service Center's general controls over automated information systems (Report Nos. 97-1-771 and 98-I-483, respectively). The audit found that of the 20 recommendations contained in the prior reports, the Bureau had implemented three recommendations, had partially implemented six recommendations, and had not implemented 11 recommendations. The most recent audit also includes one new recommendation.

The Bureau generally agrees with the findings of the followup audit. The revised corrective action plan (Attachment) provides information on the additional actions taken by the Bureau since the completion of the audit fieldwork and identifies revised target dates and officials responsible for implementing open recommendations.

Recommendation. [The Office of Inspector General] recommend[s] that the Assistant Secretary for Indian Affairs report the Bureau's ineffective general controls over its automated information systems as a material weakness in the Bureau's annual assurance statement, which is required by the Federal Managers' Financial Integrity Act.

Bureau Response. The Bureau concurs. The Bureau recognizes the security risks and is taking steps to correct these areas as we work to implement the recommendations made in the prior reports. The audit of the Center's general controls is conducted in conjunction with the OIG's audits of the financial statements of the Office of the Special Trustee for American Indians and of the Bureau of Indian Affairs and is used to evaluate the reliability of the general controls over computer-generated data that support these statements. As part of the corrective action, the Bureau is replacing the older applications systems with modem technology, which will enable more effective general controls over the automated systems.

The Trust Fund Accounting System (TFAS) that is being implemented by the Office of Trust Funds Management (OTFM) will replace the existing Individual Indian Monies system. Similarly, the

Bureau is implementing a Trust Asset and Accounting Management System (TAAMS) to replace the Land Titles and Records System and the Integrated Records Management System that comprise the Bureau's main Indian trust systems. Both systems will be operated and maintained by contractors. With the deployment of these two systems, the ability to prepare accurate and timely financial statements will be greatly enhanced.

Attachment

Attachment

STATUS OF CORRECTIVE ACTIONS FOR UNIMPLEMENTED RECOMMENDATIONS

OIG 97-I-771 General Controls Over Automated Information Systems, Operations

Service Center, BIA [Issued: April 1997]

<u>Recommendation A. 1.</u> The information technology security function is elevated organizationally to at least report to the Director, Office of Information Resources Management; is formally provided with the authority to implement and enforce a Bureauwide system security program; and is provided staff to perform the required duties, such as providing computer security awareness training and performing periodic risk assessments.

Status. The revised Departmental Manual chapter on BIA organization (130 DM 4) recognizes the Division of Information Resources Management (IRM) as providing Bureauwide information technology security leadership. Indian Affairs Manual (IAM) releases on information technology will also emphasize this point. To this end, IRM has evaluated the security plan for the Office of Law Enforcement. Regarding security awareness training, the Bureau is working with the Departmental information resources management staff to identify and develop LAN and Web based security awareness computer based training.

Revised Target Date: 12/31/99

Responsible Official: IT Security Manager

<u>Recommendation A.2.</u> Develop and document a system security program which includes the information required by the Computer Security Act of 1987 and Office of Management and Budget Circular A-l 30, Appendix III, and implement policies and procedures to keep the system security plan current.

<u>Status</u>. The Bureau of Indian Affairs Logical Security Internal Procedures Manual provides a starting point for the development of a Bureauwide security plan. The security plan and the IAM issuances will provide policies and procedures for keeping the system security program current.

Revised Target Date: 12/31/99

Responsible Official: IT Security Manager

<u>Recommendation A.3.</u> The Bureau's security personnel should perform risk assessments of the Bureau's automated information systems environment and, as appropriate, provide assurance that the necessary changes are implemented to manage the risks identified.

<u>Status</u>. It is still the Bureau's plan to initiate risk assessment in fiscal year 1999. The information security system staff will oversee the performance of the risk assessments which will be conducted in accordance with the guidance provided by OMB Circular A- 130, Appendix III, and by the General Accounting Office publication entitled "Information Security Management."

Revised Target Date:

12/31 J99

Responsible Official:

IT Security Manager

<u>Recommendation B.l.</u> Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel in sensitive or critical automated data processing positions and for informing the security staff, in writing, whenever employees who are system users terminate their employment or are transferred.

<u>Austpart</u> of a Bureauwide effort to address deficiencies in its position sensitivity and security program, all Bureau positions were reviewed and classified consistently. The Center's IT security staff is currently working on a project to bring those background investigations current with due consideration for the levels of investigation appropriate for personnel in sensitive or critical information technology positions. Policies and procedures have been drafted, and employee checkout procedures were revised to require notification of the IT security manager as part of the employee checkout process.

Revised Target Date:

1 0/3 1 /99

Responsible Official:

Bureau Security Manager

<u>Recommendation C. 1.</u> Develop and implement policies to classify the Bureau's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A- 130, Appendix III.

<u>Status</u>. It is still the Bureau's plan to begin the classification of its automated information systems in fiscal year 1999. The reviews will be done by IRM staff with the assistance of program personnel. This will be performed in conjunction with Recommendation A.3.

Revised Target Date:

12/31/99

Responsible Official

IT Security Manager

Recommendation D. 1. Sufficient staff are provided to adequately monitor all visitor activities.

<u>Status</u>. Formal procedures have been developed and issued by the Director, IRM to control visitor access into the Center. In addition, the Bureau has awarded a contract for significant improvements in access control. The improvements will include automated door control and closed circuit television subsystems.

Revised Target Date:

08/31/99

Responsible Official

IT Security Manager

<u>Recommendation D.2.</u> Provide funding for adequate maintenance of the computer operating room, such as providing daily housekeeping services, or remove fire-producing equipment and supplies from the computer room.

<u>Status</u>. The IBM 3090 and Unisys Al7 computers have been removed. The Center's daily housekeeping has been improved and the staff are no longer storing old computer equipment, records and supplies in the computer operations room. The Center has reconfigured the space to provide additional operations and storage space. This effort includes separating the area devoted to servers and tape readers from the area used for printing.

Revised Target Date: 08/01/99

Responsible Official IT Security Manager

<u>Recommendation E. 1.</u> Ensure that policies are developed and implemented which match personnel files with system users periodically, that user **IDs** are deleted from the system for users whose employment has been terminated, and that verification and approval are obtained from user supervisors and application owners or managers that the levels of access are appropriate.

<u>Status</u>. The IRM is in the process of obtaining from system owners lists of individuals who have been authorized access to the respective systems. Those individuals who have not been given access have had their user identifications deleted from the systems. To date, IRM has completed this process for the Individual Indian Monies system and the Social Services Automated System. The IRM will begin reviewing the user identifications for the Land Records Information System. All other systems will be reviewed. The IRM is also in the process of comparing user identification lists with current employee lists to eliminate those individuals no longer employed by the Bureau.

Revised Target Date: 12/31/99

Responsible Official IT Security Manager

<u>Recommendation G. 1</u>. Ensure that policies and procedures are developed and implemented which clearly identify the individuals responsible and accountable for application development and changes.

<u>TheuA</u>pplications Support Branch is responsible for developing and implementing standards, policies and procedures to ensure full accountability for all application system change management. A configuration management plan was developed for Y2K and will be expanded to cover all Bureau IT development and maintenance.

Revised Target Date: 09/30/99

Responsible Official: Chief, Applications Support Branch

<u>Recommendation H. 1.</u> Ensure that staffing at the Center is evaluated and adjusted so that the duties for critical system support functions are adequately segregated and fully utilized.

<u>ThatuBureau</u> recognizes that the required segregation of duties is a continuing challenge in an environment of reduced staffing levels and will continue to explore ways of ensuring separation of duties through its organizational changes and its assignments. For example, the Application Support Branch which performs and monitors system development is distinct from the security function which grants access to systems. Further, the individuals who control the data both by original data entry and data update are distinct from the Application Support Branch. The Bureau will continue to monitor the progress in this area.

<u>Recommendation J. 1</u>. Ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility.

<u>Status</u>. The Center is storing its backup media at the off-site storage facility. The USGS has a disaster recovery plan for the IBM mainframe and is responsible for implementing and testing the plan. The Center has a disaster recovery plan for the Unisys system and had scheduled a test of the plan on May 3 - 4, 1999. Unfortunately, the test was postponed by the contractor. The Center is in the process of rescheduling a new test date on the plan. In addition, the Bureau is developing a Continuity of Operations plan for the Center.

Revised Target Date: 06/30/99

Responsible Official: IT Security Manager

OIG 98-I-483 Followup of General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs

[Issued: June 1998]

<u>Recommendation 2</u>. Develop and approve an Office of Information Resources Management strategic plan that provides direction to and defines the functions of the Operations Service Center.

Status. The Bureau will issue the task order for the strategic and tactical plans.

Revised Target Date: 09/30/99

Responsible Official: Director, IRM

Recommendation 3. Hold the Information Technology Security Manager accountable for performing the position responsibilities

<u>Status</u>. The IT Security Manager will continue to be evaluated based upon his performance standards and position description. In addition, the IRM is in the process of augmenting its IT security staff.

<u>Recommendation 4</u>. Periodically perform an evaluation of the system security program's effectiveness and include any resultant corrective actions in future Bureau security plans.

Status The system security program will be periodically evaluated in accordance with the schedule established by the IT security plan and OMB Circular A-l 30. The first review will be completed and a periodic review schedule established by December 3 1, 1999.

Revised Target Date: 12/3 1199

Responsible Official: IT Security Manager

<u>Recommendation 5.</u> Redetermine, based on the Office of Information Resources Management's strategic plan, when the Bureau can begin performing risk assessments and classifying its resources. Also personnel who will be responsible for the risk assessments and resource classifications should be identified.

Status orrective action plan for Recommendation No. A.3

Revised Target Date: 12/31/99

Responsible Official: IT Security Manager

<u>Recommendation 6.</u> Obtain security clearances for ADP personnel who are not assigned to the Center that are commensurate with their positions.

<u>Status</u> Personnel in sensitive and critical automated data processing positions have been identified. Review and updating of background investigations of individuals who have IT system access and functions has been extended to include contractor employees, from coast to coast (including, for example contractor individuals in Washington, DC, and Portland, Oregon). The Bureau will continue to conduct and assure appropriate background investigations for individuals who enter the Bureau's work force and those who transfer from one role or location to another within the workforce.

Revised Target Date: 1 or3 1/99

Responsible Official: Bureau Security Officer

<u>Recommendation 7.</u> Require Bureau staff to review and validate the appropriateness of users' levels of access to the Bureau's IBM applications. If the users' levels of access are not reviewed and validated by Bureau personnel, the Bureau should modify its agreement with the Geological Survey to include the requirements that access reviews and verifications should be performed for the IBM applications by the Geological Survey

<u>Status</u>. The Bureau will finalize the agreement with the U.S. Geological Survey to review users' level of access.

Revised Target Date: 09/30/99

Responsible Official: Director, IRM

STATUS OF CURRENT AUDIT REPORT RECOMMENDATION

Finding/Recommendation		
Reference	Status	Action Required
1	Resolved; not implemented	No further response to the Office of Inspector General is required. The recommendation will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

STATUS OF APRIL 1997 AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
H.l and I.1	Implemented.	No further action is required.
A.l, A.2, A.3, B.1, C.l, D.l, D.2, E.1, G.l, and J.l	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations and the revised corrective action plan will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

STATUS OF JUNE 1998 AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation		
Reference	Status	Action Required
A.l, A.3, and A.8	Implemented.	No further action is required.
A.2, A.4, A.5, A.6, and A.7	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations and the revised corrective action plan will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL

Internet/E-Mail Address

www.oig.doi.gov

Within the Continental United States

U.S. Department of the Interior **Office** of Inspector General 1849 c Street, **N.W.** Mail Stop 5341 Washington, D.C. 20240

Our **24-hour** Telephone HOTLINE 1-800-424-508 1 or (202) 208-5300

TDD for hearing impaired (202) 208-2420 or 1-800-354-0996

Outside the Continental United States

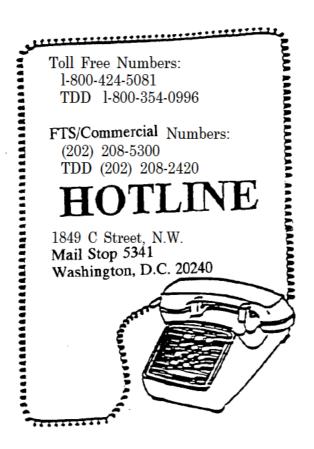
Caribbean Region

U.S. Department of the Interior Office of Inspector General Eastern Division • Investigations 4040 Fairfax Drive Suite 303 Arlington, Virginia 22203

(703) 235-922 1

North **Pacific** Region

U.S. Department of the Interior Office of Inspector General North Pacific Region 415 Chalan San Antonio Baltej Pavilion, Suite 306 Tamuning, Guam 96911 (671) 647-6060





CLOUD COMPUTING SECURITY DOCUMENTATION IN THE CYBER SECURITY ASSESSMENT MANAGEMENT SOLUTION

Report No.: 2015-ITA-017 November 2015



NOV 1 2 2015

Memorandum

To:

Sylvia Burns

Chief Information Officer

From:

Mary L. Kendall 7

au Kendall Deputy Inspector General

Subject:

Inspection Report – Cloud Computing Security Documentation in the Cyber

Security Assessment Management Solution

Assignment No. 2015-ITA-017

We inspected the completeness and adequacy of required information technology (IT) security documentation for a sample of U.S. Department of the Interior (Department) IT systems that had been moved to a public cloud. The inspection focused on: 1) whether the sampled cloud computing systems were recorded in the Cyber Security Assessment Management Solution (CSAM), and 2) if CSAM entries met Department and Federal security documentation requirements.

We sampled 16 of 26 operational systems reported by the Department: 1 from the Bureau of Ocean Energy Management, 2 from the Bureau of Safety and Environmental Enforcement, 3 from the U.S. Bureau of Reclamation, and 10 from the U.S. Geological Survey.

We issued three Notices of Potential Finding and Recommendations (NPFRs) and received bureau responses to our NPFRs' recommendations. Based on our findings, we are making seven recommendations to strengthen the Department's IT security program, and close identified security gaps.

Please provide us with your written response to this report within 30 days. The response should provide detailed information on actions you have taken or plan to take to address each recommendation, as well as target dates and titles of the officials responsible for implementing these actions. Please address your response to:

Kimberly Elmore Assistant Inspector General Office of Audits, Inspections, and Evaluations U.S. Department of the Interior Office of Inspector General Mail Stop 4428 1849 C Street, NW. Washington, DC 20240

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions regarding this report, please call me at 202-208-5745.

Table of Contents

Results in Brief	1
Introduction	2
Objective	2
Background	2
Findings	4
USBR's Documentation in CSAM is Incomplete	4
USGS's Documentation in CSAM was Incomplete	5
Cloud Computing Governance Needs Strengthening	5
Conclusion	7
Appendix 1: Scope and Methodology	8
Scope	8
Methodology	8

Results in Brief

We conducted this inspection to determine the completeness and adequacy of required information technology (IT) security documentation for 16 IT systems that the Bureaus of Reclamation (USBR), Safety and Environmental Enforcement (BSEE), and U.S. Geological Survey (USGS) had moved to a public Cloud. USBR and USGS did not meet the U.S. Department of the Interior's (Department's) policy for maintaining required IT security documentation. Specifically, USBR had not completed any security documentation for its three operational Cloud systems. As such, these systems were operating without authorization, placing bureau data in the Cloud potentially at risk of unauthorized access, disclosure, modification, or destruction.

While we found that USGS had moved its data to the Cloud in early 2013, it had not completed necessary security documentation until late 2014. These deficiences possibly occurred because the Office of Chief Information Officer (OCIO) did not effectively oversee the bureaus to ensure that operational Cloud systems met required IT security regirements.

We make seven recommendations to OCIO and affected bureaus to strengthen oversight of the Department's IT security program and close identified security gaps.

Introduction

Objective

To determine if the U.S. Department of the Interior's (Department's) security documentation for Cloud computing systems was complete by determining: 1) whether the bureaus recorded their operational Cloud systems in the Cyber Security Assessment Management system¹ (CSAM), and 2) if CSAM entries met Department and Federal security documentation requirements.

Background

A public Cloud is a shared, Internet-accessible computing environment operated by a Cloud service provider such as Amazon or Microsoft. Cloud based IT systems have the same Federal and Department security requirements as systems managed by bureau personnel and operated by a departmental data center.

As of September 2014, the Department reported it had contracted for 26 operational Cloud computer information systems. In addition, it projects significant increases in future Cloud usage, with up to 100 percent of new IT programs potentially beginning in the Cloud, and nearly all of the Department's current or legacy systems, as well as public data, likely to be moved to the Cloud.

The Department's Office of the Chief Information Officer (OCIO) requires bureaus to use CSAM as its database for information systems, including Cloud computing information systems. OCIO requires that specific security documentation for each information system be placed in CSAM.² The documentation required includes a system's security plan, security configurations, continuous monitoring strategy, contingency plans, configuration management plan, risk assessments, plan of action with milestones, and authorization decision documents.

CSAM must contain all of the Department's computer systems in order to support the annual evaluations required by the Federal Information System Management Act (FISMA).³ Systems need to have the required security information so that system owners and authorizing officials have the relevant information to support continuous monitoring, and meet the requirements of FISMA's annual assurance statements.

To help Federal agencies meet "Cloud First" requirements, the General Services Administration, in collaboration with several other agencies, established the Federal Risk Authorization Management Program (FedRAMP). FedRAMP helps

¹ The Cyber Security Assessment Management solution is a software database system used to store the Department's computer security documentation.

² Department of Interior, Office of Chief Information Officer Directive 2011-006, "Information System Boundary Assessment & Authorization Package Documentation and Inventory," March 23, 2011.

³ The Federal Information Security Management Act (FISMA) of 2002 requires an annual, independent evaluation of agencies' information security programs and practices.

agencies adopt Cloud computing technologies by (1) ensuring that Cloud providers have adequate IT security, (2) eliminating duplication of effort and reducing risk management costs, and (3) enabling rapid and cost-effective purchasing of Cloud computing services. As of June 2014, agencies are required to use only FedRAMP-approved Cloud service providers.

The Department has also mandated its Cloud First policy. The Department is transitioning from owning and operating its entire IT infrastructure to using Cloud services. The January 2014 Cloud First policy memorandum notes the Department's "Cloud Strategy" is key to transforming the Department's IT capabilities into a modern Cloud based environment. Central to this strategy is the use of a Department contracting vehicle for future IT hosting procurements. The goal is to reduce the total cost of ownership of enterprise hosting hardware, software, and IT operations; and to provide greater service, security, and end-user support.

OCIO oversees bureau compliance for using CSAM. The Internal Control, Audit, and Compliance Management Division (ICACMD) in OICO is responsible for ensuring that bureaus meet Department and Federal information technology security requirements.

-

⁴ Memorandum from Chief Information Officer and Director of the Office of Acquisition and Property Management and Senior Procurement Executive, Subject: Mandatory Use Policy for the Department of the Interior Foundation Cloud Hosting Services Contracts, dated January 6, 2014.

Findings

Of the 16 cloud computing systems we reviewed during our inspection, we found no security documentation for the 3 USBR systems, complete but not timely documentation for the 10 USGS systems, and complete and timely documentation for the 3 BOEM/BSEE systems. Not having complete and timely documentation for these cloud systems not only doesn't meet the requirements of FISMA's annual assurance statements, but places Bureau data at risk of unauthorized access, disclosure, modification, or destruction. We believe the Department's OCIO plays a key role in ensuring cloud systems compliance, and as such, needs to strengthen its oversight in this area.

USBR's Documentation in CSAM is Incomplete

The Bureau of Reclamation (USBR) operated three Cloud computing systems without any security documentation or records placed in CSAM. USBR security managers stated that they were unaware of these systems; consequently, they had not done proper security planning, completed required security documents, or formally authorized the systems for operation. Accordingly, USBR's Cloud computing systems could be subject to unauthorized access, modification, or undetected destruction.

USBR shared one of its Cloud systems with eight other entities, including Federal, State, county, and tribal units. USBR personnel stated they were not aware of which entity had security responsibilities, or if security responsibilities were shared. FedRAMP specifies how to implement a shared Cloud computing system among several agencies. Specifically, one of the agencies acts as a sponsor and is then responsible for obtaining an authorization to operate. The other participating agencies may choose to leverage the sponsoring agency's authorization to operate, or conduct their own security assessment work.

USBR's noncompliance with FedRAMP occurred because the responsible USBR officials said they had not conducted security planning and documentation, and, therefore, had not placed security documentation in CSAM as required. We issued a "Notice of Potential Findings and Recommendations" (NPFR) to USBR with three recommendations. USBR concurred with the recommendations that were in the NPFR and that follow.

Recommendations

We recommend that USBR's Chief Information Security Officer:

- Prepare the appropriate security documentation for existing and planned Cloud computing systems, grant authority to operate as appropriate, and ensure required documents are added to CSAM.
- 2. Review FedRAMP for guidance, roles, and responsibilities when multiple Federal agencies implement a shared Cloud computing service.
- Ensure all planned and operational Cloud computing services are reported to OCIO's ICACMD.

USGS's Documentation in CSAM was Incomplete

USGS combined its 10 Cloud systems into one CSAM boundary⁵ because of their design and use. The Cloud computing systems were operational in 2013, but USGS did not timely update CSAM with a full set of security documents until December 2014. CSAM now contains the appropriate documentation.

We made one recommendation to USGS in an NPFR concerned with services reported to OCIO's ICACMD (see Recommendation 4 below). USGS concurred with this recommendation and noted that it has developed new internal processes for ensuring Cloud computing systems meet security requirements, and that it now has sufficient documentation within CSAM.

Recommendation

We recommend that USGS:

4. Ensure all planned and operational Cloud computing services are timely reported to OCIO's ICACMD.

Cloud Computing Governance Needs Strengthening

Overall, OCIO does not have adequate oversight of the Department's security documentation for Cloud systems. It is important for all departmental systems to have the required security information so that system owners and system authorizing officials can support continuous monitoring and annual assurance statements. If CSAM is incomplete, then the annual FISMA evaluation may misrepresent the status of the Department's security program. The deficiencies we identified occurred because neither the responsible bureaus nor the Department's

⁵ Computer security boundaries are a set of systems under a single administrative control.

officials ensured that their Cloud computing systems met Federal and Department security protocols. In particular, Department security personnel need to better understand FedRAMP's stated roles and responsibilities when collaborating with other agencies.

We issued an NPFR to OCIO that contained four recommendations to help ensure bureau compliance with Federal and Department IT security requirements, and to strengthen OCIO oversight of bureau practices related to Cloud computing. OCIO concurred with two recommendations directing bureaus to update CSAM and review FedRAMP roles and responsibilities to ensure Cloud systems meet applicable IT security requirements.

Based on OCIO's response to our other two preliminary recommendations, we withdrew one, which required bureaus to biannually report to OCIO all planned and operational Cloud computing systems as OCIO already requires such reporting. Finally, we reworded our last recommendation to strengthen the Department's IT governance by having OCIO reevaluate and enhance its IT security oversight practices.

Recommendations

We recommend that OCIO: direct responsible Bureau information technology staff to:

- 5. Update CSAM for all planned and operational Cloud computing systems.
- 6. Review specific FedRAMP roles and responsibilities for authorizing Cloud computing systems.

We recommend that OCIO:

 Direct ICACMD to reevaluate and enhance its oversight, monitoring, and testing processes, to include periodic reviews to ensure bureaus comply with OCIO Directive 2011-006.

Conclusion

The bureaus need to evaluate systems to ensure they are following Federal guidelines, including FedRAMP. They have the responsibility to upload current and accurate security documentation into CSAM. OCIO needs to monitor CSAM regularly to ensure the bureaus timely upload the required security documentation. Although ICACMD oversees this area, it must improve its oversight to ensure a complete inventory is maintained. For example, our findings show that the current practice of bureau self-reporting Cloud systems is ineffective and increases the risk of unauthorized access to Department Cloud systems. In addition, the Department must keep an accurate inventory to have the required security information so that system owners and system authorizing officials have the relevant information to support continuous monitoring and, most importantly, meet the requirements of FISMA's annual assurance statements.

As a result of OMB's Cloud First policy, the Department has also implemented a mandatory policy to move IT into a modern Cloud based environment. The Department's goal is to reduce the total cost of owning enterprise hosting hardware, software, and IT operations, while providing greater service, security, and end-user support.

Our findings relating to deficiencies in operating Cloud systems show the need for the Department to strengthen its governance over Cloud systems to ensure that the Department meets its IT security requirements for this new paradigm. The bureaus need to improve uploading security documentation into CSAM and OCIO needs to improve its oversight of the bureaus' use of CSAM.

Appendix I: Scope and Methodology

Scope

We limited our inspection to a judgmental sample of 16 of the 26 operational Cloud information systems reported by the U.S. Department of the Interior.

Methodology

The Department's policy for using the Cyber Security Assessment Management system (CSAM) specifies that each computer system's security documentation must be posted in CSAM. Required documentation includes the system's security plan, security configurations, continuous monitoring strategy, contingency plans, configuration management plan, risk assessments, plan of action with milestones, and authorization decision documents. We identified each of the sampled Cloud systems in CSAM, and looked at their documentation to assure that the documents met Federal and departmental requirements.

We conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

We interviewed bureau and Department staff to determine the processes and guidance they were following. We reviewed the DOI Cloud First policy and Federal policy documentation to determine best practices.

⁶ Department of Interior Office of Chief Information Officer Directive 2011-006, "Information System Boundary Assessment & Authorization Package Documentation and Inventory," March 23, 2011.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



U.S. DEPARTMENT OF THE INTERIOR'S MANAGEMENT OF ITS SMARTPHONES, TABLETS, AND OTHER MOBILE DEVICES



JUN 2 2 2016

Memorandum

To:

Sylvia Burns

Chief Information Officer

From:

Mary L. Kendall Mary Kindall

Deputy Inspector General

Subject:

Final Audit Report – U.S. Department of the Interior's Management of its

Smartphones, Tablets, and Other Mobile Devices

Report No. 2015-ITA-032

This report transmits the results of our audit of mobile computing device management. We reviewed whether the U.S. Department of the Interior (DOI) effectively managed costs by adopting an enterprise-wide approach for procuring and managing its portfolio of mobile computing devices, limiting the number of mobile computing devices issued, and monitoring usage to ensure public funds are not spent on unused mobile devices. We also assessed the adequacy of DOI's implemented controls to mitigate security risks unique to mobile computing devices.

We identified weaknesses in DOI's mobile device management practices that have resulted in DOI spending tens of thousands of dollars on unused mobile devices. We found that DOI did not have a complete inventory of its mobile devices and services and did not implement a Departmentwide approach for procuring and managing these devices. In addition, we found that some of DOI's mobile computing devices do not have proper security configurations, which could result in unauthorized access to Government systems and data by cybercriminals.

We offered four recommendations to help DOI improve its management and security of mobile computing devices. In its response to our draft report, the Office of the Chief Information Officer (OCIO) concurred with two recommendations and did not concur with two recommendations (see Appendix 3). Based on OCIO's response, we consider three recommendations resolved but unimplemented and one recommendation unresolved (see Appendix 4). We will refer all four recommendations to the Office of Policy, Management and Budget to track their implementation and resolution.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, evaluation, and inspection reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions regarding this report, please call me at 202-208-5745.

Table of Contents

Results in Brief	1
Introduction	2
Objective	2
Background	2
DOI's Use of Mobile Devices	3
Findings	5
Bureau Spending on Unused Mobile Devices Exceeds \$600,000 Annual	ly 5
Inadequate Enforcement of Required Security Controls Puts Sensitive D Thousands of Mobile Computing Devices at High Risk of Loss	
Conclusion and Recommendations	10
Conclusion	10
Recommendations Summary	10
Appendix 1: Scope and Methodology	12
Scope	12
Methodology	12
Appendix 2: Monetary Impact	14
Appendix 3: Response to Draft Report	15
Appendix 4: Status of Recommendations	22

Results in Brief

Mobile computing devices, such as smartphones and tablets, are key components of the U.S. Department of the Interior's (DOI) information technology (IT) strategy. These devices allow employees access to DOI data and systems from anywhere at any time, as well as the ability to store large amounts of data. DOI spends approximately \$16.5 million each year on at least 35,576 mobile devices. The benefits mobile devices afford, however, can also be the greatest risk. Because they are small, hand-held, and portable, mobile devices that are not physically secured by the user are highly vulnerable to theft, loss, and damage

We found that DOI did not have a complete inventory of its mobile devices and services and did not implement a Departmentwide approach for procuring and managing these devices. As a result, DOI has spent hundreds of thousands of dollars on unused mobile devices. We reviewed mobile usage and inventory data for the four DOI bureaus that had the most Government-issued mobile devices: Bureau of Land Management (BLM), National Park Service (NPS), U.S. Fish and Wildlife Services (FWS), and U.S. Geological Survey (USGS). As a result of our analysis of usage data from October 1, 2014, to March 30, 2015, we found that the four bureaus spent \$50,470 a month on 1,557 unused mobile devices.

In addition, we found that thousands of DOI's mobile computing devices do not have proper security configurations, which could result in unauthorized access to Government systems and data by cybercriminals. The National Institute of Standards and Technology recommended that organizations enroll mobile devices in an enterprise-wide management solution to ensure required security controls and usage policies are implemented on the devices before they are issued to employees. As of June 2015, we found that DOI had not enrolled thousands of devices issued by the four bureaus in the Departmentwide mobile device management solution. This deficiency could result in potential security breaches, as these devices are vulnerable to unauthorized access by cybercriminals.

As DOI employees increasingly rely on tablet computers and smartphones to perform their jobs, it is imperative that DOI improve the inventory, acquisition, issuance, use, monitoring, and securing of its mobile computing devices. Full implementation of our recommendations by DOI's Chief Information Officer will help DOI improve its management and security of mobile computing devices.

1

¹ An enterprise-wide management solution is one that encompasses centralized management of mobile devices across the entire organization as a whole rather than having each office or department separately manage its devices.

Introduction

Objective

We reviewed mobile computing device management at the U.S. Department of the Interior (DOI) to determine whether DOI effectively managed costs by adopting an enterprise-wide approach for procuring and managing its portfolio of mobile computing devices, limiting the number of mobile computing devices issued, and monitoring usage to ensure public funds are not spent on unused mobile devices. We also assessed the adequacy of DOI's implemented controls to mitigate security risks unique to mobile computing devices. Appendix 1 provides further details of our scope and methodology.

Background

According to the U.S. Government Accountability Office (GAO), Federal agencies spend about \$1.2 billion annually on mobile computing devices and services. Mobile computing devices are key components of the Government's information technology (IT) strategy, offering employees the flexibility to access systems and data from anywhere at any time. The U.S. Office of Management and Budget (OMB) requires Federal agencies to use an enterprise-wide approach for procuring and managing mobile computing devices to reduce costs and improve the ability to track mobile device usage, secure devices, and deliver mobile applications.² Federal agencies are also required to maintain mobile device inventories, monitor usage, and establish controls to ensure that public funds are not spent on unused or underutilized mobile devices.³

While mobile devices with computing capabilities⁴ offer greater workplace flexibility, these devices are also susceptible to security compromise because of their size, portability, constant wireless connection, physical sensors, and location services. Moreover, the diversity of available devices, operating systems, carrier-provided services, and applications used on the devices present additional security challenges. Finally, despite their small size, mobile devices can store large amounts of data.

The Federal Chief Information Officer Council identified the top security threats for mobile devices and suggested mitigation strategies (see Figure 1). ⁵ The Council recommended that Federal agencies implement an enterprise-wide mobile device management solution that allows users to securely access Government resources while protecting the services and data accessed.

² "Digital Government: Building A 21st Century Platform To Better Serve The American People," OMB, May 23, 2012.

³ Executive Order 134589, "Promoting Efficient Spending," November 2011.

⁴ Mobile devices with computing capabilities refer to smartphones and tablet computers.

⁵ The Federal Chief Information Officer Council and U.S. Department of Homeland Security, "Mobile Security Reference Architecture," May 23, 2013.

Common Threats	Mitigation Strategies
 Insecure configuration Unauthorized access Virus and malware Loss of sensitive data Device loss or theft 	 Device management Password to unlock device User training Encryption of data Remote wipe of DOI applications and data

Figure 1. Common Threats and Mitigation Strategies for mobile devices.

Source: The Federal Chief Information Officer Council and U.S. Department of Homeland Security, "Mobile Security Reference Architecture," May 23, 2013.

DOI's Use of Mobile Devices

DOI spends about \$16.5 million annually on approximately 35,576 mobile computing devices, including smartphones and tablet computers. DOI's mobile devices can store large amounts of data, despite their small size, with storage capabilities of up to 32 gigabytes for smartphones and up to 64 gigabytes for tablets.

DOI employees and contractors are approved to use two different operating systems:

- Android: Android is a Linux-based operating system developed by Google for mobile phones and tablets. The open-source nature of Linux allows individual users to tailor this operating system to meet his or her needs, which provides varying security risks.
- iOS: Apple developed iOS as the operating system for its iPhones and iPads.

To effectively secure and remotely manage its portfolio of mobile devices, DOI's Office of the Chief Information Officer (OCIO) selected MaaS360 as its mobile device management solution. MaaS360 is a commercial device management platform that can ensure devices have security configurations that are in compliance with DOI's IT security policy.⁶

At the time of our audit, GAO conducted a Governmentwide review of mobile device management practices. GAO's review included the U.S. Fish and Wildlife Service (FWS) and the National Park Service (NPS). GAO issued a report in May 2015, offering three recommendations to help DOI effectively manage spending on mobile devices and services. ⁷ GAO recommended that DOI:

⁶ U.S. Department of the Interior OCIO Memorandums, "Risk Acceptance for the Use of Apple iPads, iPhones, iOS 5, and iTunes Desktop/Laptop Application Suite," June 7, 2012; and "Risk Assessment for Google Android Operating System and Android Hardware," November 16, 2012.

^{7 &}quot;Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services," GAO-15-431, May 2015.

- 1) ensure an inventory of mobile devices and services is established Departmentwide (i.e., all components' devices and associated services are accounted for);
- 2) ensure a reliable Departmentwide inventory of mobile service contracts is developed and maintained; and
- 3) ensure procedures to monitor and control spending are established Departmentwide. Specifically, ensure that
 - i. procedures include assessing devices for zero, under, and over usage;
 - ii. personnel with authority and responsibility for performing the procedures are identified; and
 - iii. the specific steps to be taken to perform the process are documented.

DOI concurred with GAO's recommendations, and DOI's written response included planned actions to address each recommendation. Some of our findings related to inventory management and device usage are similar to GAO's. Therefore, we did not make recommendations that duplicate those already made. Our audit, however, also quantified overspending by DOI on unused mobile devices and included IT security findings.

Findings

As the use of mobile devices to conduct daily operations continues to increase, DOI must improve its governance and security controls over mobile devices in order to recognize cost savings and bolster IT security. We found that DOI spends approximately \$600,000 a year on unused mobile devices at the four bureaus we reviewed: Bureau of Land Management (BLM), U.S. Geological Survey (USGS), FWS, and National Park Service (NPS), U.S. Fish and Wildlife Service (FWS), and U.S. Geological Survey (USGS). Moreover, DOI's decentralized approach for purchasing mobile devices and services is inefficient and hinders DOI from reducing costs by leveraging its buying power with service providers.

Furthermore, we found that thousands of mobile devices did not have the security configurations installed as mandated by the OCIO, which could result in unauthorized access to Government data, especially if these devices are lost or stolen. In addition, if a cybercriminal accesses an unsecure mobile device, the criminal could use data on the device to gain unauthorized access to DOI networks and systems. We believe these deficiencies occurred because DOI did not—

- 1. maintain an inventory of its mobile devices and had not developed or implemented effective policies and procedures to govern the acquisition, issuance, use, and monitoring of mobile devices and services; and
- 2. enroll mobile devices in its mobile device management solution to ensure the required security controls and usage polices had been implemented before issuing the devices to employees.

Bureau Spending on Unused Mobile Devices Exceeds \$600,000 Annually

Executive Order requires Federal agencies to maintain inventories, monitor device usage, and establish controls to ensure that public funds are not spent on unused or underutilized mobile devices. We analyzed Verizon usage data from October 1, 2014, to March 30, 2015—the most recent time period that usage data were available—and found that BLM, FWS, NPS, and USGS spent \$50,470 per month (for 1 or more months) on 1,557 unused mobile devices (see Figure 2), resulting in approximately \$600,000 per year. Assuming that the bureaus continue with the current cellular plans for the next 3 years, spending on unused mobile devices would exceed \$1.7 million based on the 3-year discount rate established by the Office of Management and Budget (see Appendix 2).

We also identified 486 activated mobile devices at the four bureaus that had zero usage for the 3-month period that ended September 2014 (see Figure 3). Prolonged periods of zero usage may indicate that the bureaus issued mobile

_

⁸ Executive Order 134589, "Promoting Efficient Spending," November 2011.

devices to employees without a valid business need or that devices were lost or stolen but unreported.

Bureau	Unused Mobile Devices as of March 2015	Total Plan Amount
BLM	803	\$16,049
FWS	213	\$9,874
NPS	381	\$17,513
USGS	160	\$7,034
Total	1,557	\$50,470

Figure 2. Unused Verizon mobile devices as of March 30, 2015. Source: OIG Analysis of Verizon Wireless data provided by DOI.

Bureau	Unused Mobile Devices since 2014
BLM	116
FWS	108
NPS	184
USGS	78
Total	486

Figure 3. Devices that have not been used since the 3-month period that ended September 2014.

Source: OIG Analysis of Verizon Wireless data provided by DOI.

Based on the scope of our review, which included only four bureaus and only devices using Verizon as the service provider, we believe that the amount of overspending and number of unused devices Departmentwide is certainly higher. We did not have access to comparable data from DOI's other wireless service providers. We also could not determine the total percentage of mobile devices and related services supplied by Verizon because not all of the four bureaus we reviewed maintained a complete inventory of mobile devices and related service plans.

We believe that expenditures on unused mobile devices occurred because the four bureaus we reviewed did not maintain an inventory of their mobile devices and had not developed or implemented effective policies and procedures to govern the acquisition, issuance, use, and monitoring of mobile devices and services. For example, the bureaus did not monitor usage to determine whether employees had a continuing business need for mobile devices. Moreover, DOI did not implement an enterprise-wide approach for procuring and managing its portfolio of mobile computing devices as required by OMB. Instead, we found that program managers procure and manage devices locally. As a result, DOI may waste

⁹ In addition to Verizon, DOI also uses AT&T, Sprint/Nextel, T-Mobile, and U.S. Cellular as wireless service providers.

Government funds on unused mobile devices. Until DOI implements measures to more effectively manage its mobile devices, it is likely that public funds will continue to be misspent on unused mobile devices.

Recommendations

We recommend that DOI:

- Implement the recommendations GAO made in May 2015 to help DOI effectively manage spending on mobile devices and services; and
- 2. Implement an enterprise-wide approach for procuring and managing DOI mobile devices.

Inadequate Enforcement of Required Security Controls Puts Sensitive Data on Thousands of Mobile Computing Devices at High Risk of Loss

Forty-one percent of data breaches result from the loss of mobile computing devices, so it is imperative to have adequate security controls to help protect the sensitive data stored on these devices. ¹⁰ To effectively secure and remotely manage its portfolio of mobile devices, DOI's OCIO selected MaaS360 as its mobile device management solution. MaaS360 is a commercial device management platform that can remotely apply and manage security configurations. In addition to secure configurations, MaaS360 also provides device encryption, secure password settings, and the ability to remotely locate, lock, and delete all data on lost or stolen mobile devices. Although MaaS360 is a Departmentwide requirement, each bureau or office must ensure that its mobile devices comply with DOI's IT security policy. ¹¹

In addition, the National Institute of Standards and Technology recommended that organizations enroll devices in an enterprise-wide device management solution (e.g., MaaS360) to ensure required security controls and usage polices were implemented before issuing the devices to employees. ¹²

As of June 2015, we found that MaaS360 did not manage thousands of mobile computing devices issued by the four bureaus (see Figure 4). Our analysis did not include flip phones, as these devices do not have computing capabilities.

¹⁰ TrendMicro Inc., "Follow the Data: Dissecting Data Breaches and Debunking the Myths," September 22, 2015.

¹¹ U.S. Department of the Interior OCIO Memorandums, "Mandatory Deployment of the Department of the Interior Enterprise System for All Bureaus and Offices," March 15, 2012; "Risk Acceptance for the Use of Apple iPads, iPhones, iOS 5, and iTunes Desktop/Laptop Application Suite," June 7, 2012; and "Risk Assessment for Google Android Operating System and Android Hardware," November 16, 2012.
¹² National Institute of Standards and Technology Special Publication SP-800-124 Rev. 1, "Guidelines for Managing the Security of Mobile Devices in the Enterprise," June 2013.

Bureau	Smart- phones	Tablets	Smart- phones and Tablets	Smartphones and Tablets Managed by MaaS360	Percent Managed by MaaS360
BLM	2,533	883	3,416	2,630	77%
FWS	2,505	235	2,740	2,096	77%
NPS	3,801	585	4,386	2,716	62%
USGS	2,085	118	2,203	1,298	59%
Total	10,924	1,821	12,745	8,740	69%

Figure 4. Verizon mobile computing devices used by the four bureaus managed by MaaS360 as of June 2015.

Source: OIG Analysis of Verizon Wireless data provided by DOI.

Devices not managed by MaaS360 can still be used to login to any DOI system that is accessible over the Internet from a web browser. This includes Gmail and related Google applications (e.g., Google Drive, Google Documents, etc.). In addition, device users may potentially download gigabytes of information from DOI systems, including files with sensitive data, to their unencrypted smartphones or tablets. As such, we found that the absence of required security controls potentially compromises thousands of DOI mobile devices to unauthorized access if the devices are lost or stolen. Further, the extent of the potential security breach is not limited to the compromised mobile device. For example, a cybercriminal in control of an unprotected mobile device could potentially use information on it (e.g., user names and passwords) to gain unauthorized access to DOI's computer networks and systems.

The loss or theft of a mobile computing device is a security incident that is recorded in a Departmentwide incident tracking system. Unfortunately, because the system has limited reporting capabilities, we were unable to determine the number of lost or stolen mobile computing devices that may put sensitive Government data at risk to unauthorized access.

We found that the four bureaus did not follow the recommended best practice of enrolling mobile devices in MaaS360 before issuing the devices to employees. Instead, the bureaus issued activated and fully functional smartphones and tablet computers to employees along with instructions for how to enroll the device in MaaS360 and enable key security controls (e.g., data encryption, strong passwords, location services etc.). The bureaus did not verify if employees had enrolled their Government-issued mobile devices in MaaS360 to comply with OCIO's security policy. Therefore, thousands of DOI mobile devices are not adequately secured or centrally managed.

We believe the total number of mobile computing devices Departmentwide without the required security controls is higher than reported because our analysis included only four bureaus and was limited to mobile devices with a Verizon Wireless service plan. In addition, our analysis did not include tablet computers that did not have a separate wireless plan and instead access the Internet using a WiFi connection.

Unless DOI improves its practices for managing security controls on its mobile devices, sensitive data on thousands of unencrypted DOI mobile devices will remain at high risk of unauthorized access.

Recommendations

We recommend that DOI:

- Verify that its mobile device management solution (e.g., MaaS360)
 manages all mobile devices distributed to employees and contractors;
 and
- 4. Enroll newly acquired mobile devices in to DOI's mobile device management solution before issuing the devices to individual users.

Conclusion and Recommendations

Conclusion

DOI faces a significant challenge to implement enterprise-wide mobile device management practices. Without a complete inventory of mobile devices and services and a Departmentwide approach for procuring these devices, DOI will continue to pay for unused mobile devices and will be unable to ensure that all mobile devices are adequately secure. Further, DOI must enroll these devices in its mobile device management solution (e.g., MaaS360) to help protect against unauthorized access. As the use of mobile computing technologies expands and becomes more advanced, DOI must continually strengthen its governance and risk management practices to prevent the misuse of Government funds and help mitigate adverse effects if these devices are lost or stolen.

Recommendations Summary

We recommend that DOI:

1. Implement the recommendations GAO made in May 2015 to help DOI effectively manage spending on mobile devices and services.

OCIO Response: In its response to our draft report, OCIO concurred with this recommendation. OCIO stated that efforts are underway to resolve and implement the recommendations GAO made in May 2015.

OIG Comment: Based on OCIO's response, we consider this recommendation resolved but unimplemented until OCIO satisfactorily addresses all three pre-existing GAO recommendations. We will refer this recommendation to the Office of Policy, Management and Budget (PMB) to track implementation.

2. Implement an enterprise-wide approach for procuring and managing DOI mobile devices.

OCIO Response: OCIO concurred with this recommendation, stating that efforts are underway, through contract action and associated policies and procedures, to implement the recommendation.

OIG Comment: Based on OCIO's response, we consider this recommendation resolved but unimplemented. We will refer this recommendation to PMB to track implementation.

3. Verify that DOI's mobile device management solution (e.g., MaaS360) manages all mobile devices distributed to employees and contractors.

OCIO Response: OCIO did not concur with this recommendation, stating that not all mobile devices are candidates for enrollment in DOI's mobile device management solution. OCIO stated that certain mobile devices, which are not data-consumption devices, cannot be managed using the mobile device management solution and are managed using DOI's standard client management tools.

OIG Comment: Our reference to mobile devices in the report chapter and related recommendation pertains to mobile devices with computing capabilities (e.g., smartphones and tablet computers) and not to mobile devices that provide only cellular telecommunication services (e.g., flip phones). We recognize that flip phones are not data-consumption devices and thus cannot be managed using DOI's mobile device management solution. We reiterate that departmental policy requires all iPhone, iPad, and android devices provided by DOI and connecting to DOI's network to be managed using MaaS360, DOI's enterprise-wide solution for mobile device management. Moreover, departmental policy does not mention any other approved mobile device management solutions besides MaaS360. Based on OCIO's response, we consider this recommendation unresolved. We will refer this recommendation to PMB for resolution.

4. Enroll newly acquired mobile devices in to DOI's mobile device management solution before issuing the devices to individual users.

OCIO Response: OCIO did not concur with this recommendation, stating that not all mobile devices are candidates for enrollment in the mobile device management solution. OCIO stated, however, that DOI will issue a clarifying directive that mobile devices that process DOI data must be secured in accordance with the National Institute of Standards and Technology Special Publication SP 800-124 Revision 1 within 72 hours of being issued to individual users.

OIG Comment: Our reference to mobile devices in the report chapter and related recommendation pertains to mobile devices with computing capabilities (e.g., smartphones and tablet computers) and not to mobile devices that provide only cellular telecommunication services (e.g., flip phones). We recognize that flip phones are not data-consumption devices and cannot be managed using DOI's mobile device management solution. As such, we consider OCIO's planned actions responsive to our recommendation. We consider the recommendation resolved but unimplemented and will refer it to PMB to track implementation.

Appendix I: Scope and Methodology

Scope

We focused on determining whether the U.S. Department of the Interior (DOI) effectively managed costs by adopting an enterprise-wide approach for procuring and managing its portfolio of mobile computing devices, limited the number of mobile computing devices issued, and monitored device usage to ensure public funds were not spent on unused and underutilized mobile devices. We also assessed internal controls related to the security of DOI's mobile computing devices. We reviewed DOI and bureau policies, procedures, and practices for management of mobile devices throughout their lifecycle, mobile usage patterns, and device inventories. We reviewed mobile usage and inventory data for the four bureaus that issued the most mobile devices: Bureau of Land Management, National Park Service, U.S. Fish and Wildlife Service, and U.S. Geological Survey.

We conducted this audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

Methodology

DOI does not have a complete and accurate inventory of all mobile devices; therefore, to determine whether DOI effectively managed mobile devices, we requested and obtained from DOI third-party usage data for DOI's main mobile device provider, Verizon Wireless, which according to the DOI Contracting Officer, accounts for approximately 80 percent of all DOI spending on mobile devices and services. Using the Verizon Wireless usage data for October 1, 2014, through March 31, 2015, we analyzed the usage of mobile devices to determine the number, percentage, and cost of various devices with zero usage in voice or data. We traced the unused mobile devices to usage data that covered the 3 months ended September 30, 2014, and identified the activated mobile devices at the four bureaus that had zero usage for extended periods. In addition, we compared this data to the inventories of all devices that are managed in DOI's mobile device management solution in the same time period to determine whether all mobile devices managed by DOI are included in the mobile device management solution and therefore have the security controls in place required by the Office of the Chief Information Officer (OCIO).

To accomplish our objectives, we reviewed relevant Federal laws and regulations; DOI, bureau, and office policies and procedures; information related to lifecycle management of mobile devices from the bureaus and offices; usage data from vendors; and enrollment data in DOI's mobile device management solution; and

interviewed management and responsible officials from OCIO and the bureaus to understand the nature of the mobile device solution and controls implemented.

We used computer-processed data from the third-party provider, Verizon Wireless. We reviewed the Verizon usage data from October 1, 2014, through March 31, 2015. To assess the completeness and accuracy of this data, we compared the inventory listing of DOI Office of Inspector General (OIG) employees to the Verizon data and ensured that the OIG employees were included in the Verizon dataset for this time period. We chose OIG because we could verify the completeness and accuracy of OIG's inventory due to our familiarity with the office, because it centrally procures mobile devices, and because it maintains a complete and accurate inventory.

Appendix 2: Monetary Impact

We found that the U.S. Department of the Interior (DOI) spent at least \$600,000 a year on unused mobile computing devices as of March 2015. The following table summarizes our estimate of potential savings DOI could realize over the next 3 years through more effective management of its mobile computing devices.

After we sent the Notifications of Potential Findings and Recommendations—which are usually issued before the audit work is completed and when some or all of the critical elements of a finding still require development—to the related bureaus, OCIO raised concerns, which it reiterated in its response to our draft report (see Appendix 3). Specifically, OCIO stated that our calculation of overspending on unused devices in our preliminary findings included lines of service that were not associated with DOI. Before issuing our draft report, we reviewed each record in the Verizon data set and excluded those records that were not associated with a DOI bureau or office. The overspending amounts we provided in the draft and final reports were based on the data set from which we removed all records for non-DOI entities.

Assuming that the bureaus would continue their current cellular plans, we calculated potential savings (present value) over the next 3 years by multiplying the total annual cost by the 3-year discount rate established by the Office of Management and Budget. Because our review included only four bureaus and was limited to one cellular service provider, Verizon Wireless, we believe our savings estimate is conservative.

	Identified Savings (Questioned Costs)	Potential Savings Over Next 3 years (Funds to be Put to Better Use)
Unused mobile devices	\$605,646	\$1,763,423

Appendix 3: Response to Draft Report

The Office of the Chief Information Officer's response follows on page 16.



United States Department of the Interior

OFFICE OF THE SECRETARY Washington, DC 20240

MAR 3 0 2016

MEMORANDUM

To:

Mary L. Kendall

Deputy Inspector General

From:

Sylvia Burns, Chief Information Officer

Subject:

Office of the Chief Information Officer Response to Draft Audit

Report, U.S. Department of the Interior's Management of its Smartphones,

Sylvin B

Tablets, and Other Mobile Devices, Report No. 2015-ITA-032

The Office of the Chief Information Officer (OCIO) for the Department of the Interior appreciates the opportunity to review the Office of the Inspector General (OIG) Draft Audit Report. We have discussed the recommendations with the impacted bureaus (USGS, FWS, NPS, and BLM). Pursuant to your request, the OCIO submits the attached *Statement of Actions* for implementation of the OIG's recommendations as noted in the draft report.

If you have any questions, please contact me at (202) 208-6194. Staff may contact Steven B. Thompson, Acting Director, Compliance and Audit Management (CAM) at (202) 821-8887.

cc:

Alexandra Lampros, Financial Specialist, Office of Financial Management Steven B. Thompson, Acting Director, Compliance and Audit Management

Kristen Sarri, DAS-PMB

Elena Gonzalez, DAS-TIBS, PMB

Olivia Ferriter, DAS-BFPA, PMB

Amy Holley, Chief of Staff, PMB

Debra Sonderman, PAM

Denise Flanagan, POB

Douglas Glenn, PFM

Alexandra Lampros, PFM

Steven B. Thompson, OCIO

Mark Sogge, USGS

Tim Quinn, USGS

Alan Wiser, USGS

Ken Taylor, USFWS

Susan Gabriel-Smith, BLM

Shane Compton, NPS

DOI ADIRS

OCIO ELT

Attachments:

1. OCIO Statement of Actions to Address Office of Inspector General Draft Audit Report U.S. Department of the Interior's Management of its Smartphones, Tablets, and Other Mobile Devices, Report No. 2015-ITA-032

Office of the Chief Information Officer Statement of Actions to Address Office of Inspector General Draft Audit Report U.S. Department of the Interior's Management of its Smartphones, Tablets, and Other Mobile Devices, Report No. 2015-ITA-032

Background and Observations

The Department of the Interior (DOI) relies heavily on a broad array of mobile and cellular devices and services to fulfill our mission objectives and to support the health and safety of our employees. The DOI Office of the Chief Information Officer (OCIO) supports these activities by coordinating with leadership across the organization to: (1) establish policies, processes and controls to ensure the appropriate stewardship of mission data and government resources; and (2) establish and support mandatory use, DOI-wide contracts and shared services to optimize the appropriate and efficient utilization of mobile devices and services across the enterprise.

The OCIO and named bureaus each received two Notices of Potential Findings and Recommendations (NPFRs) in summer, 2015, related to the OIG Mobile Computing Device Management Audit (OIG 2015-ITA-032). The first concerned "unused" mobile devices. This Finding is provided in the Draft Audit Report.

Inventory of Mobile Devices and Services

As evidenced by our comprehensive cellular wireless initiatve, which includes plans for an enterprise acquisition mechanism and associated policy and procedural changes, DOI agrees that the Department needs to better manage its cellular devices and services.

However, the magnitude of the financial impact estimated in this Draft Audit Report may be materially overstated due to the scope and quality of the data underpinning the Audit. Our specific concerns regarding the data include the following:

- State Wildlife agency lines of service identified as US Fish and Wildlife Service (FWS);
- State district attorneys and the Oklahoma Department of Human Services lines of service identified as US Geological Survey (USGS);
- Confirmed "Terminated" lines of service appeared in the report;
- Confirmed "Suspended" lines of service appeared in the report;
- Verizon disclaimed the information provided, stating that the data "was neither audited nor verified."

The Department further asserts that retaining "unused" and "ready-to-use" mobile devices may be both necessary and prudent to fulfill mission and legal requirements including but not limited to: wildland fire management, law enforcement, support for rotating seasonal workforce, records retention and legal discovery.

Security of Mobile Devices

The second NPFR issued to the OCIO and named bureaus pertained to the security of mobile devices themselves. This Finding and its associated Recommendations, numbers three and four, are also presented in the Draft Audit Report. The OCIO agrees with the spirit of the Recommendations, but respectfully submits that it cannot concur with them as written. Not all mobile devices are candidates for enrollment in the Department's mobile device management (MDM) solution. Nor is it necessary or fiscally responsible to maintain one-to-one parity of device inventory with MDM licensing and enrollment counts. Bureaus and offices routinely have legitimate business reasons for maintaining un-provisioned devices. Similarly, certain mobile devices cannot be managed using the Department's MDM solution, and are managed instead using the Department's standard client management tools, and/or are not data consumption devices. Figures and device totals presented in support of the Finding do not appear to take these conditions into account. DOI has committed to secure mobile devices that process DOI data in accordance with the Guidelines provided in National Institute of Standards and Technology (NIST) Special Publication 800-124 Revision 1, which is footnoted in the Draft Audit Report on page 7.

Response to Recommendations

<u>Recommendation 1</u>: Implement the recommendations GAO made in May 2015 to help DOI effectively manage spending on mobile devices and services.

Response: OCIO concurs with the recommendation. The GAO made three recommendations in their Report, "Telecommunications: Agencies Need Better Controls to Achieve Significant Savings on Mobile Devices and Services, GAO-15-431, May 2015. They are:

- 1. Ensure the establishment of a Department-wide inventory of mobile devices and services (i.e., all components' devices and associated services are accounted for)
- 2. Ensure a reliable Department-wide inventory of mobile service contracts is developed and maintained
- 3. Ensure Procedures to Monitor and Control Spending are established Department-wide. Specifically, ensure that:
 - Procedures include assessing devices for zero, under, and over usage;
 - Personnel with Authority and Responsibility for Performing the Procedures are Identified; and
 - The specific steps to be taken to perform the process are documented.

As DOI has indicated in its response to the GAO, efforts are underway to resolve and implement each of these three audit recommendations. In order to eliminate duplicate effort and unnecessarily duplicative administrative requirements, DOI requests clarification of this Recommendation, recognizing that it should be addressed and reported exclusively by reference to the associated and pre-existing GAO Audit Recommendation.

Responsible Official & Title: Jerry Johnston, Director, Information and Technology Management Division

Lead Contact & Title: Andrew Havely, Chief, Solutions Design and Innovation

Target Completion Date: Resources Permitting: 12/31/2016 (the same as the current target completion dates of all three GAO audit recommendations)

<u>Recommendation 2</u>: Implement an enterprise-wide approach for procuring and managing DOI mobile devices.

Response: OCIO concurs with the recommendation. Efforts are underway to resolve and implement this recommendation through contract action and associated policies and procedures for the utilization of cellular devices and services.

Responsible Official & Title: Jerry Johnston, Director, Information and Technology Management Division

Lead Contact & Title: Andrew Havely, Chief, Solutions Design and Innovation

Target Completion Date: Resources Permitting: 12/31/2016 (the same as the current target completion dates of all three GAO audit recommendations)

<u>Recommendation 3</u>: Verify that DOI's mobile device management solution (e.g., MaaS360) manages all mobile devices distributed to employees and contractors.

Response: OCIO cannot concur with the recommendation as written. Not all mobile devices are candidates for enrollment in the Department's mobile device management (MDM) solution. Similarly, certain "mobile devices" cannot be managed using the Department's MDM solution, and are managed instead using the Department's standard client management tools, and/or are not data consumption devices. Nor is it necessary or financially responsible to maintain one-to-one parity of device inventory with MDM licensing and enrollment counts: Bureaus and offices have legitimate business reasons for keeping certain unprovisioned devices and lines of service active for rapid redistribution or transfer when cancellation and new cellular service activation would otherwise negatively impact the mission.

The Department will secure mobile devices that process DOI data in accordance with the Guidelines provided in NIST SP 800-124 Revision 1. We recommend, and can concur with, this language in the final report.

Responsible Official & Title: Karen Matragrano, Acting Director, Service Delivery Division

Lead Contact & Title: Trent Randall, Unified Messaging Chief, End User Services Branch

Recommendation 4: Enroll newly acquired mobile devices into DOI's mobile device management solution within 72 hours of issuing the devices to individual users

Response: OCIO cannot concur with the recommendation as written. Not all mobile devices are candidates for enrollment in the Department's mobile device management solution. However, the Department will issue a clarifying directive that mobile devices that process DOI data are to be secured in accordance with the Guidelines provided in NIST SP 800-124 Revision 1 within 72 hours of issuance to individual users. We recommend, and can concur with, this language in the final report.

Responsible Official & Title: Lawrence Ruffin, DOI Chief Information Security Officer

Lead Contact & Title: Chris Rutherford, DOI Deputy Chief Information Security Officer

Appendix 4: Status of Recommendations

In its response to our draft report, the Office of the Chief Information Officer (OCIO) concurred with two recommendations and did not concur with two recommendations (see Appendix 3). OCIO's response also included an action official for each recommendation and target dates for the two recommendations with which it concurred. Based on the response, we consider three recommendations resolved but unimplemented and one recommendation unresolved.

Recommendations	Status	Action Required
I, 2, and 4	Resolved but unimplemented.	We will refer these recommendations to the Office of Policy, Management and Budget to track implementation.
3	Unresolved.	We will refer this recommendation to the Office of Policy, Management and Budget for resolution.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



INFORMATION TECHNOLOGY SECURITY WEAKNESSES AT A CORE DATA CENTER COULD EXPOSE SENSITIVE DATA

This is a revised version of the report prepared for public release.

Report No.: 2016 ITA 021 February 2017



FEB 1 5 2017

Memorandum

To: Sylvia Burns

Chief Information Officer

Lawrence S. Roberts

Assistant Secretary - Indian Affairs

From: Mary L. Kendall

Deputy Inspector Genera

Subject: Final Evaluation Report - Information Technology Security Weaknesses at a Core

Kudall

Data Center Could Expose Sensitive Data

Report No. 2016-ITA-021

We conducted an evaluation to assess the effectiveness of select information technology security controls for protecting the Department of the Interior's and the computer systems it houses from potential loss or disruption. We offer eight recommendations to help ensure that DOI data centers and the systems they house are adequately secured.

In response to our draft report, the Office of the Chief Information Officer concurred with our eight recommendations. We consider seven recommendations resolved but not implemented and one recommendation resolved and implemented. We will refer these recommendations to the Office of Policy, Management and Budget for tracking and resolution.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, evaluation, and inspection reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions regarding this report, please call me at 202-208-5745.

Table of Contents

Results in Brief	1
Introduction	2
Objective	2
Background	2
CDM Program	3
Findings	<i>6</i>
Incomplete Hardware Asset Inventories	(
Software Asset Management Control Not Implemented	7
Thousands of Unmitigated Critical and High-Risk Vulnerabilities on High-Value IT Assets	7
Computer Servers Not Securely Configured	9
Ineffective Contingency Planning Practices Resulted in Temporary Lo of Data Center Availability	
Weak Oversight of Bureau and Contractor IT Security Practices	12
Conclusion and Recommendations	14
Conclusion	14
Recommendation Summary	14
Appendix 1: Scope and Methodology	18
Scope	18
Methodology	18
Appendix 2: Response to Draft Report	20
Appendix 3: Status of Recommendations	27

Results in Brief

The Continuous Diagnostics and Mitigation (CDM) program is a dynamic approach to fortifying the cyber security of Government networks and systems. including those of the U.S. Department of the Interior (DOI). We previously evaluated DOI's CDM program in our report, "U.S. Department of the Interior's Continuous Diagnostics and Mitigation Program Not Yet Capable of Providing Complete Information for Enterprise Risk Determinations" (Report No. ISD-IN-MOA-0004-2014-I). In this evaluation, we found that the CDM program at DOI's is immature and not fully effective in protecting the 24 information technology systems owned by the Bureau of Indian Affairs (BIA) and the Bureau of Indian Education (BIE) from potential exploitation. We also assessed the adequacy of controls that help ensure continuity of business experience a disaster. operations should We found that BIA's management practices failed to detect critical and high-risk vulnerabilities on the an high-value IT asset that contains personally identifiable information

high-value IT asset that contains personally identifiable information and left thousands of critical and high-risk vulnerabilities unmitigated for years on other BIA and BIE systems. In addition, BIA's capability to identify unauthorized computers or detect and remove obsolete and potentially malicious software (i.e., malware) were inadequate, exposing systems to potential compromise. BIA also did not monitor any of its computers to ensure they remained securely configured over time. We also found that inadequate contingency planning for resulted in temporary disruption to DOI and other Federal agencies' mission operations due to a power outage in March 2016.

These deficiencies occurred because BIA failed to: (1) install DOI's inventory management software on all computers; (2) identify and remove unauthorized and unsupported products from BIA and BIE systems; (3) mitigate vulnerabilities in a timely manner; (4) monitor its contractors to ensure all IT security requirements were met; (5) monitor computers to ensure they remained securely configured; and (6) meet annual contingency planning and plan testing requirements. Further, the Office of Chief Information Officer (OCIO) did not provide the oversight necessary to ensure that BIA complied with the Department's IT security program. Until BIA improves its IT security practices and OCIO strengthens its oversight role, BIA high-value IT assets will remain at high risk of compromise, the results of which could have a serious adverse effect on DOI operations and cause the loss of sensitive data. We make seven recommendations to BIA and one recommendation to OCIO to help ensure that DOI data centers and the systems they house are adequately secured.

Introduction

Objective

We assessed the effectiveness of selected information technology (IT) security controls for protecting the U.S. Department of the Interior's (DOI)

and the computer systems it houses from potential loss or disruption. Specifically, we assessed progress in—

- developing inventories of computer hardware and software;
- managing operating system configurations; and
- detecting and mitigating technical vulnerabilities.

These are key elements for the foundation of an organization's IT security program and the Phase 1 requirements for the governmentwide Continuous Diagnostics and Mitigation (CDM) initiative. We also assessed the adequacy of controls that help ensure continuity of business operations should experience a disaster.

Background

DOI spends about \$1 billion annually on its information technology asset portfolio, which include data centers and the computer systems they house that support a range of bureau programs that—

- protect and manage our Nation's natural resources and cultural heritage;
- provide scientific and other information to stakeholders interested in those resources; and
- help meet responsibilities to American Indians, Alaska Natives, and affiliated Island communities.

A DOI data center is a facility used for housing and protecting computer systems
and communications equipment that store and process data used to support bureau
operations. is one of the Department's . As such,
operates 24 computer systems that support the mission of the bureaus of Indian
Affairs and Indian Education. also houses computer systems used by other
bureaus and Federal agencies. Indian Affairs is responsible for overall
management of the and the BIA Chief Information Security Officer is
responsible for ensuring the implementation of the Department's IT security
program for BIA and BIE systems operated at
DOI designated as well as one of the computer systems it houses—the
as high-value IT assets.
According to the U.S. Office of Management and Budget (OMB), high-value IT
assets refer to those IT systems, facilities, and data that are of particular interest to
nation-state adversaries, such as foreign military and intelligence services.

Specifically, high-value IT assets often contain sensitive data or support mission-critical operations. The loss or disruption of a high-value IT asset could have a serious adverse effect on agency operations, assets, or individuals.

CDM Program

Established by Congress in 2013, the CDM program is a dynamic approach to fortifying the cyber security of Government networks and systems. Specifically, as noted in OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems," dated November 18, 2013, CDM provides Federal agencies with capabilities and software tools that identify cyber security risks on an ongoing basis and prioritize these risks based on potential impacts, enabling IT personnel to mitigate the most significant problems first. CDM also provides risk-based and cost-effective cyber security capabilities to more efficiently allocate limited cyber security resources.

The CDM program spans 15 continuous diagnostic control areas that will be implemented in three phases. Phase 1 is the foundation for protecting Federal information systems and data by using automated software tools to help agencies establish and maintain computer hardware and software inventories and implementing enterprise wide vulnerability and configuration management capabilities. We previously evaluated DOI's CDM program in our report, "U.S. Department of the Interior's Continuous Diagnostics and Mitigation Program Not Yet Capable of Providing Complete Information for Enterprise Risk Determinations" (Report No. ISD-IN-MOA-0004-2014-I).

An organizationwide inventory of computers and software programs is a fundamental control that helps Federal agencies ensure that only authorized computers and approved software are present in each agency's IT environment. Moreover, accurate hardware and software inventories also increase the effectiveness of an IT security program by certifying that 100 percent of an organization's IT assets undergo continuous monitoring to ensure they remain securely configured and free of vulnerabilities.

Vulnerabilities. Vulnerabilities are software flaws or system misconfigurations that can be exploited to gain access to or control of an information system. Vulnerability scanners are specialized software programs that automate the vulnerability detection process. Specifically, vulnerability scanners search large databases of known vulnerabilities associated with commonly used computer operating systems and software applications. When a match is found in the database, the scanner alerts the operator to a possible vulnerability. The scanners rank vulnerabilities according to their potential to harm the system, allowing an organization to prioritize and mitigate its most critical vulnerabilities. Most vulnerability scanners also generate reports to help system administrators fix discovered vulnerabilities. System administrators commonly remediate vulnerabilities by applying software patches, updating a system configuration, or

adding a compensating control. DOI's IBM BigFix repository also contains vulnerability data for the systems monitored.

Configuration management is the process of assessing and, if necessary, modifying settings to ensure that such IT assets as computer servers and clients (e.g., workstations and laptops) remain in a secure state, with security configurations implemented and set, and are not vulnerable to exploitation. Often, operating systems on these computers are configured by the vendor for ease-of-deployment and ease-of-use rather than for security, leaving them exploitable in their default state. To address this issue, the Center for Internet Security (CIS) has published recommended configuration settings, called benchmarks, for securing a wide variety of computer operating systems. We used the CIS benchmark to measure compliance with best practices in our testing.

Initializing a computer's operating system to a secure state is not sufficient to ensure ongoing protection against exploitation. As such, ongoing configuration monitoring is essential for maintaining the security of the Department's high-value IT assets. For example, computer operating systems that are improperly configured are susceptible to compromise and thus may potentially be used by intruders to gain unauthorized access to the Department's computer network. Once inside, the intruder can use the compromised computer to exploit other weaknesses, which could result in the loss or impairment of Department IT resources, including its high-value IT assets. Because operating system configurations can change when software patches are applied or when computers are upgraded, it is necessary to monitor operating systems continuously to verify that they remain securely configured.

Data centers and the computer and communication systems they house are vulnerable to a variety of disruptions such as power outages, hardware failures, or equipment destruction resulting from fire or other catastrophic events. Contingency planning defines the resources needed and processes to be followed in order to effectively and efficiently recover a system following a disruption. If a disruption occurs and the contingency plan is not effective, the organization could be unable to perform critical business operations. Thus, contingency planning and contingency plan testing helps mitigate the risk to business operations by providing assurance that the data center and the computer and communication systems it houses will be recoverable and normal operations can be restored following a disruption.

The Federal Information Modernization Act of 2014 (FISMA) defines specific information security requirements Federal agencies, including DOI, must satisfy and assigns responsibilities to agency heads, senior agency officials, and agency inspectors general for satisfying FISMA requirements. FISMA requires that agencies develop policies and procedures commensurate with the risk and magnitude of harm resulting from the malicious or unintentional impairment of agency information assets. Under FISMA, the Department's Chief Information

Officer (CIO) is responsible for developing and overseeing departmentwide, risk-based, and cost-effective program for meeting Federal and departmental IT security requirements.

Independent verification and validation (IV&V) is a structured, two-step quality control and quality assurance process widely used for improving products and processes in the information technology domain. Verification, the first step, determines whether a product or process meets regulations. Validation, the second step, establishes evidence to provide a high degree of assurance that a product or process meets its intended requirement.

Findings

Based on our review of Continuous Diagnostics and Mitigation (CDM) and contingency planning practices at the we found that the Bureau of Indian Affairs' (BIA) CDM program ineffective for protecting the 24 BIA and Bureau of Indian Education (BIE) systems at loss or disruption. Specifically, we found that the bureaus either failed to implement all four CDM Phase 1 controls, or implemented the control incompletely or ineffectively. We also found that BIA's poor contingency planning practices contributed to computer hardware failures at adversely affected mission operations for BIA, the Office of the Special Trustee and the U.S. Department of Health and Human Services when their information technology (IT) systems housed at became unavailable. Overall, our findings reflect that the Office of the Chief Information Officer (OCIO) does not provide effective oversight of bureaus and cannot ensure that bureaus fully implement the Department's IT security program.

Incomplete Hardware Asset Inventories

The goal of the CDM hardware asset management control is to actively inventory and track all hardware devices, such as computers, routers, and firewalls, so that only authorized devices are present in the Department of the Interior's (DOI) IT environment. As part of implementing this control, DOI selected IBM BigFix software as its enterprisewide solution for managing hardware and software inventories. In order to develop inventories of authorized hardware devices and approved software products, IBM BigFix agents (software programs) must first be installed on all DOI computers. Once installed, the agents register DOI computers and the software programs on them to a central repository. The repository serves as an authoritative departmentwide hardware and software inventory. The data in the repository are used for reporting key IT security metrics to senior DOI and Office of Management and Budget (OMB) officials, which help allocate resources and shape future IT security investments.

We performed discovery scans at using network addresses supplied by BIA and BIE. We identified 793 BIA network devices and 209 BIE network devices representing either a computer, firewall appliance or other network device. For BIA, we tested 185 of the 793 devices (23 percent) to determine whether the devices were included in the Department's hardware inventory. We found that 22 of the 185 devices (12 percent) were not included in the hardware inventory because DOI's hardware inventory management solution (IBM BigFix) had not been installed on those devices ¹. BIA IT security personnel stated that the IBM BigFix software was not installed on the 22 devices because the systems associated with them were either test systems or under development. BIA IT staff thought only computers and network devices that were part of production systems

6

¹ We provided the specific details of our scan results to the BIA Chief Information Security Officer after completion of our tests.

needed to have the Department's inventory management software installed on them

None of the 209 BIE devices (computers, firewalls etc.) at were included in the Department's hardware inventory because the Department's inventory management solution had not been installed on them. This occurred because Indian Affairs, which includes both BIA and BIE, did not fund the purchase of IBM BigFix licenses for BIE systems. According to the BIA Chief Information Security Officer, BIE purchased IBM BigFix software licenses and installation on all BIE IT assets is projected to be completed by April 2017.

OCIO requires that all bureaus and offices load IBM BigFix agents on 100 percent of supported workstations, servers, and devices. This hardware asset inventory control is critical to the overall effectiveness of DOI's CDM program. For example, without a complete and accurate hardware inventory, DOI cannot demonstrate that 100 percent of the applicable devices connected to its networks undergo continuous monitoring to ensure the devices are securely configured and free of critical and high-risk vulnerabilities. A system breach of 1 of the 24 moderate impact systems at could result in the disruption of mission-critical bureau operations and could also result in the loss of sensitive data. Moreover, CDM reports will be inaccurate as they will be based on incomplete information, which could lead to a misrepresentation of the security status of DOI's high-value IT assets and a misallocation of resources.

Software Asset Management Control Not Implemented

We found that BIE did not implement the software asset management control because the IBM BigFix software needed to develop the software inventory was not installed on any BIE computers. This occurred as previously stated, because Indian Affairs did not provide the necessary funding to BIE to acquire the IBM BigFix software licenses.

To quantify the risk to systems, including the high-value IT asset we tested computers for the presence of vulnerabilities including those associated with unsupported or potentially malicious software. Our tests confirmed the presence of unsupported software containing hundreds of critical and high-risk vulnerabilities on BIA and BIE computers. Upon completion of our tests we provided the details of these vulnerabilities to BIA for remediation.

Thousands of Unmitigated Critical and High-Risk Vulnerabilities on High-Value IT Assets

Detecting and mitigating vulnerabilities before they can be exploited are essential
for protecting DOI's high-value IT assets from loss or disruption. We found that
the contractor hired by BIE to operate the
had not implemented the Department's vulnerability

management process for a high-value IT asset containing sensitive information including personally identifiable information (PII)

We also found that BIA and BIE left thousands of critical and high-risk vulnerabilities unmitigated for years. These deficiencies occurred because Indian Affairs did not—

- effectively oversee the contractor responsible for implementing required security controls on
- promptly mitigate discovered vulnerabilities; and
- mitigate vulnerabilities associated with unsupported software by either removing the software or upgrading to a newer version.

Moreover, because neither BIA nor BIE have complete inventories of computers, the bureaus cannot ensure that vulnerability detection and mitigation process was applied to 100 percent of the computers connected to its networks. As a result, some BIA and BIE computers may not undergo vulnerability scanning and thus, may contain undetected and uncorrected vulnerabilities.

We tested 1,002 BIA and BIE devices at using the credentials of privileged user accounts provided by bureau representatives. The hardware devices we tested included computer servers, workstations, and other network devices, such as firewalls and routers, as discovered.

Although the OCIO's security policy requires that bureaus mitigate all critical and high-risk vulnerabilities within 30 days of detection, our tests found over 20,000 unmitigated critical and high-risk vulnerabilities on BIA and BIE's IT assets (see Figure 1). Almost 4,000 of the vulnerabilities we detected remained unmitigated for years, even though software patches to fix the vulnerabilities were available. We found a total of 13,430 instances of vulnerabilities on 337 Microsoft Windows workstations and servers, some of which date back to 2009. We provided the details of these vulnerabilities to BIA for remediation.



Unmitigated Critical and High-Risk Vulnerabilities

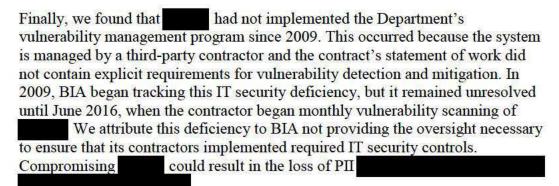
Bureau	Number of Devices Tested	Critical and High- Risk Vulnerabilities Detected	Critical and High- Risk Vulnerabilities With Available Software Patches
BIA	793	14,441	2,388
BIE	209	5,694	1,584
Total	1,002	20,135	3,972

Figure 1. We identified 20,135 unmitigated critical and high-risk vulnerabilities on DOI's high-value IT assets, including 3,972 with available software patches. Source: OIG analysis of DOI data.

unapplied for more than one year.

We also found hundreds of critical and high-risk vulnerabilities on BIA and BIE computers associated with software programs that were no longer supported by the vendor, and accordingly, no longer receive software updates or security patches. Unlike vulnerabilities associated with supported software programs, vulnerabilities present on unsupported software can only be remediated by removing the software or by upgrading to a newer version. As a result, these vulnerabilities will remain unmitigated until the software is either removed or upgraded.

Compromising DOI's high-value IT assets by exploiting any of the thousands of vulnerabilities we detected could have a serious adverse effect on bureau operations and result in the loss of sensitive data.



Computer Servers Not Securely Configured

To help organizations validate that their computers are securely configured the Center for Internet Security (CIS) developed an automated scoring tool (the CIS Configuration Assessment Tool). Using the CIS Configuration Assessment Tool, we tested 14 Windows servers and 4 Windows workstations at BIA and the 6 BIE

servers that store and process data. For the BIA computers tested the computer servers were 90 percent compliant and the workstations were 76 percent compliant with the related CIS secure baseline settings. The servers tested, however, were only 42 percent complaint with recommended CIS benchmark settings.

According to BIA officials, the servers were put into production before securely configuring the operating system because the contract did not specifically require the contractors to do so. National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," requires agencies to define secure configuration settings for all of its IT systems, including those managed by third parties.

Servers were not securely configured because OCIO did not provide adequate oversight to ensure BIE met Federal and Department IT security requirements. As such, servers were susceptible to compromise, which could result in the disruption of Indian School operations and in the loss of sensitive data.

Finally, we found that neither BIA nor BIE monitored operating system configuration settings to ensure computers remained securely configured over time. This occurred on BIA managed systems because OCIO did not mandate computer operating system configuration monitoring even though configuration monitoring is a recommended best practice and IBM BigFix provides the capability. Operating system configurations were not monitored because BIA's contract did not require it. Without ongoing configuration monitoring, DOI increases the risk that computers operating high-value IT assets could be compromised—which could potentially have a serious or adverse effect on DOI operations, assets, and individuals.

During our review, we learned that OCIO is developing secure baselines for its operating systems and requiring that bureaus configure their operating systems using the baselines. OCIO is also requiring bureaus to monitor computer operating systems to ensure they remain securely configured. OCIO set a deadline of June 30, 2018, for departmentwide implementation of these two new security measures.

Recommendations

We recommend that BIA:

- Establish an ongoing process to ensure the inventory of its systems is continually updated and accurate;
- 2. Install IBM BigFix agents on all applicable BIA and BIE devices;
- Implement controls that identify and remove unauthorized and unsupported products from BIA and BIE systems;
- Ensure that critical and high risk vulnerabilities on BIA and BIE systems are mitigated within 30 days of detection in accordance with DOI policy;
- Review contracts for BIA and BIE systems managed by contractors to ensure the contract contains the appropriate Federal computer security requirements, including critical IT security controls such as vulnerability detection and mitigation;
- Monitor contractors managing BIA and BIE systems to ensure all IT security requirements are met; and
- 7. Monitor system configuration settings to ensure BIA and BIE systems remain securely configured over time.

Ineffective Contingency Planning Practices Resulted in Temporary Loss of Data Center Availability

Proper planning and preparation for potential disruptions to the imperative to ensure that BIA, BIE, and external customers can perform mission operations without interruption. For example, NIST 800-34-rev1 "Contingency Planning Guide for Federal Information Systems," May 2010, requires that Federal agencies develop contingency plans for data centers and the systems they house and test the plans at least annually. Contingency plan development and annual plan testing helps ensure continuity of data center operations in the event of a disruption.

During a power outage on March 14, 2016, we found that inadequate contingency planning and plan testing resulted in computer hardware failures at and loss of system availability of BIA, the U.S. Department of Health and Human Services (HHS), and the Office of the Special Trustee (OST) systems. A power outage at a utility substation affected about 4,500 customers including Loss of power to the data center triggered the successful "failover" to generators and

power was immediately restored to computers in the data center; however, power was not immediately restored to the computer room air conditioning units. As a result, the temperature in reached 120 degrees Fahrenheit within an hour, causing computer hardware failures and loss of system availability. Power was not restored to computer room air conditioning units when generators came on line because the electrical switch that connects the air conditioning units to the generators was set to "OFF." The incorrect setting was not identified until approximately an hour later, at which point power was returned to the computer room air conditioning units.

The computer hardware failures and temporary loss of system availability could have been avoided had met Federal requirements for contingency planning and plan testing. For example we found that had not tested its contingency plan for more than 2 years. Moreover, contingency plan tests for three other moderate impact systems housed by also were not tested annually, as required. A disruption to or the 24 moderate-impact systems it houses can result in loss of system availability and have serious to serious adverse effect on BIA, BIE, HHS, and OST operations.

A March 24, 2016 After Action Report of the power outage includes corrective actions to improve contingency planning and plan testing practices. A contingency plan test for was performed in October 2016. Because the After Action Report identifies corrective actions to mitigate deficiencies, we will not issue any recommendations for contingency planning and plan testing activities.

Weak Oversight of Bureau and Contractor IT Security Practices

In our judgement, OCIO could have discovered the deficiencies we identified in BIA's IT security program had it implemented processes to verify and validate bureaus' compliance with Federal and departmental IT security requirements. As a result, the CIO is not receiving timely and accurate information with which to evaluate and report to the Office of Management and Budget the status of its IT security program.

We believe that establishing an independent validation and verification function within OCIO, could strengthen the Department's security program by improving internal processes, which could help ensure that Federal and Department IT security requirements are met. Without this oversight function, DOI cannot ensure that: (1) IT security controls adequately safeguard Department data centers and the systems and data they house; (2) data centers and the systems they house can be effectively recovered and normal operations can be restored following a disruption; and (3) contractors entrusted with implementing security controls for DOI systems and data meet Federal and Department IT security requirements.

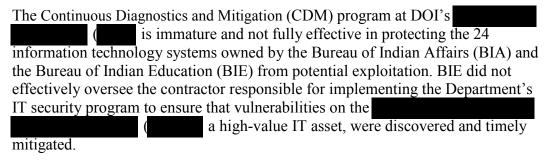
Recommendation

We recommend that OCIO:

8. Establish an independent verification and validation function to ensure that all Federal and Department IT security requirements are met and its data centers and the information systems they house are adequately secured.

Conclusion and Recommendations

Conclusion



Bureau management practices left thousands of critical and high-risk vulnerabilities unmitigated for years on other BIA and BIE systems. BIA and BIE computers are running vulnerable unsupported software because the Department has not established and enforced approved software lists. These vulnerabilities cannot be readily mitigated because vendor-provided software patches are no longer available. We also found that contingency planning practices contributed to a hardware failures that temporarily affected the availability of BIA, BIE, the Office of the Special Trustee, and Department of Health and Human Services systems.

These deficiencies occurred because BIA failed to: (1) install DOI's inventory management software on all computers; (2) identify and remove unauthorized and unsupported products from BIA and BIE systems; (3) mitigate vulnerabilities in a timely manner; (4) monitor its contractors to ensure all IT security requirements were met; (5) monitor computers to ensure they remained securely configured; and (6) meet annual contingency planning and plan testing requirements. Further, in our judgement, these deficiencies occurred because the Office of the Chief Information Officer (OCIO) did not provide the necessary oversight to ensure that bureaus and their contractors met Federal and Department IT security requirements. OCIO's IT security program would benefit from an independent verification and validation function for its IT security program. Such a program would improve OCIO's internal process and reduce the risk of compromise to DOI's high-value IT assets.

Recommendation Summary

We recommend that BIA:

1. Establish an ongoing process to ensure the inventory of its systems is continually updated and accurate.

BIA Response: BIA concurred with our recommendation. BIA will document a process to ensure that the inventory of its systems is continually updated and accurate. Target completion date is June 30, 2018.

OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to the Office of Policy, Management and Budget (PMB) to track its implementation.

2. Install IBM BigFix agents on all applicable BIA and BIE devices.

BIA Response: BIA concurred with our recommendation. BIA will install BigFix agents on all applicable devices. Target completion date is June 30, 2018.

OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

3. Implement controls that identify and remove unauthorized and unsupported products from BIA and BIE systems.

BIA Response: BIA concurred with our recommendation. BIA is implementing CDM phase 1 controls that will incorporate capabilities for software asset management controls. Target completion date is June 30, 2019.

OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

4. Ensure that critical and high-risk vulnerabilities on BIA and BIE systems are mitigated within 30 days of detection in accordance with DOI policy.

BIA Response: BIA concurred with our recommendation. BIA is implementing CDM phase 1 controls that will incorporate capabilities and processes for vulnerability management. Target completion date is June 30, 2018.

OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

5. Review contracts for BIA and BIE systems managed by contractors to ensure the contract contains the appropriate Federal computer security requirements, including critical IT security controls such as vulnerability detection and mitigation.

BIA Response: BIA concurred with our recommendation. Indian Affairs reviewed the Statement of Work and determined that the overarching security requirements are included. In addition, BIA produced a guidance document to reset expectations with the contractor regarding security

and privacy controls and more clearly define deliverables and reporting requirements that support those controls. This document will be shared with other BIA and BIE Contracting Officers for use in support of future Indian Affairs contracts. Indian Affairs considers this recommendation resolved and implemented.

OIG Reply: We noted BIA's prompt action to resolve this recommendation as a result of findings from our evaluation. Based on BIA's response and review of the guidance document, we consider this recommendation resolved and implemented.

6. Monitor contractors managing BIA and BIE systems to ensure all IT security requirements are met.

BIA Response: BIA concurred with our recommendation. As of July 2016, Indian Affairs receives monthly vulnerability scanning reports from the contractor. Indian Affairs considers this recommendation resolved and implemented.

OIG Reply: We agree with BIA's directing the contractor to implement the Department's vulnerability management process. BIA's response, however, did not mention actions taken to ensure that monthly credentialed vulnerability scans for the entire population of computers are consistently performed. As such, we consider the recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

7. Monitor system configuration settings to ensure BIA and BIE systems remain securely configured over time.

BIA Response: BIA concurred with our recommendation. BIA is implementing CDM phase 1 controls that will incorporate capabilities and processes to monitor configuration settings to ensure computers remain securely configured. Target completion date is June 30, 2018.

OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. We will refer this recommendation to PMB to track its implementation.

We recommend that OCIO:

8. Establish an independent verification and validation function to ensure that all Federal and Department IT security requirements are met and its data centers and the information systems they house are adequately secured.

OCIO Response: OCIO concurred with our recommendation. The Compliance and Audit Management (CAM) Branch is the OCIO's

independent verification and validation for closing IT audit recommendations and conducts FISMA compliance reviews using independent auditors and other assessments across bureaus and offices within DOI. OCIO considers this action complete.

OIG Reply: Based on the information provided, we consider this recommendation resolved, but not yet implemented. OCIO has not provided evidence that bureau data centers and the information assets they house are independently evaluated to ensure that Federal and Department IT security requirements are met. As such, we consider the recommendation resolved but not yet implemented. We will refer this recommendation to PMB to track its implementation.

Appendix I: Scope and Methodology

Scope

The objective of this evaluation was to assess the effectiveness of security controls for Phase 1 of the governmentwide Continuous Diagnostics and Mitigation initiative. We performed technical testing of the computer networks and systems and evaluated selected physical security controls.

For this evaluation, our work was limited to the specific procedures and analysis described in the "Rules of Engagement" completed with the Bureau of Indian Affairs (BIA), and was based only on the information made available through June 29, 2016.

Our testing did not include third-party customer systems because their data and applications are owned by the third parties and not the Department.

Methodology

To accomplish our evaluation objectives, we—

- conducted interviews with subject matter experts at the Office of the Chief Information Officer, BIA, and the Bureau of Indian Education;
- performed a walkthrough of
- reviewed system security documentation for a sample of systems;
- developed scripts and network tests for on-site testing to obtain systemspecific data; and
- compared the results of our technical tests with the data in IBM BigFix.

We obtained a listing of Department-owned assets hosted at judgmentally selected three systems for detailed testing. We selected our sample based on the FIPS 199 security categorizations of "Moderate" and systems rated highest for having sensitive data, quantity of sensitive information controlled or handled, uniqueness of the dataset or capability, impact of loss or compromise, system dependencies, communication support, and type of risk in the event the system is compromised.

from April 25, 2016 through April 29, 2016, and from June 28, 2016 through June 29, 2016. We based initial assessment targets on a range of Internet-Protocol (IP) addresses provided by BIA for Department-owned assets at Using the IP ranges provided, we performed discovery tests for common services. Responding IP addresses were then scanned for vulnerabilities with administrative rights. We configured automated tools with "safe" settings so they would not directly impact services.

We then reviewed the automated testing results for relevancy and accuracy. We reported technical findings that presented a significant concern to warrant

additional evaluation and mitigation by BIA and BIE in separate technical vulnerability assessment reports.

As part of our technical testing, we used NESSUS®, an automated vulnerability detection tool to test computers and network devices for vulnerabilities, such as computers running outdated or unpatched software or network services with known security weaknesses. NESSUS® ranks vulnerabilities as critical, high, moderate, or low based on their potential to harm the system.

We asked BIA and BIE to provide workstation and server configurations and deviations. Then, we used automated tools to determine whether the devices were adequately configured.

We also per	rformed walkthroughs of conducted interviews with
security and	d data center operations personnel, evaluated selected physical security
controls of	the data center, and reviewed system security plans, contingency
plans, and	backup site documentation.

We conducted this evaluation in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of Inspectors General on Integrity and Efficiency. We believe that the work we performed provides a reasonable basis for our conclusions and recommendations.

Appendix 2: Response to Draft Report

The Office of the Chief Information Officer's response follows on page 21.



United States Department of the Interior

OFFICE OF THE SECRETARY Washington, D.C. 20240

JAN 0 6 2017

To:

Kimberly Elmore

Assistant Inspector General for Audits, Inspections, and Evaluations

From:

Chief Information Officer

Lawrence S. Roberts

Principal Deputy Assistant Secretary - Indian Affairs

Subject:

Office of Inspector General, Information Technology Security Weaknesses at the

U.S. Department of the Interior's Core Data Center Could Expose Sensitive Data,

Draft Evaluation Report No. 2016-ITA-021, November 2016

The Department of the Interior (Department), Bureau of Indian Affairs (BIA) and the Office of the Chief Information Officer (OCIO), appreciate the opportunity to respond to the Office of Inspector General (OIG) Draft Evaluation Report (Report), Information Security Weaknesses at the U.S. Department of the Interior's Core Data Center Could Expose Sensitive Data, 2016-ITA-021. Attachment 1 provides the Department's planned corrective actions to implement the OIG's recommendations and serves as our formal response.

The BIA and OCIO on behalf of the Department, fully cooperated with the OIG since being advised of this evaluation. The Department accepts the OIG's recommendations and has engaged the BIA to develop the planned corrective action responses for recommendations 1 through 7 and engaged the appropriate OCIO program areas to develop planned corrective action response for recommendation 8.

The Department appreciates the OIG's evaluation of this data center and its objective perspective on this aspect of the Department's IT security posture in the interest of promoting excellence, integrity, and accountability in our IT program, operations, and management.

If you have any questions, please contact me at (202) 2086194 or sylvia burns@ios.doi.gov. Staff may contact Richard Westmark, Chief, Compliance and Audit Management (CAM) at (202) 513-0749, or richard westmark@ios.doi.gov.

cc:

Allen Lawrence, Office of Financial Management (PFM), Chief, Internal Control and

Audit Follow-up (ICAF) Branch Alexandra Lampros, PFM, ICAF,

Richard Westmark, Chief, Compliance and Audit Management Branch

Attachment:

 Joint Bureau of Indian Affairs (BIA) and Office of the Chief Information Officer (OCIO) Statement of Actions Planned to Address Office of Inspector General (OIG) Draft Evaluation Report - Information Technology Security Weaknesses at the U.S. Department of the Interior's Core Data Center Could Expose Sensitive Data, Draft Report No. 2016-ITA-021

Attachment 1

Joint Bureau of Indian Affairs (BIA) and Office of the Chief Information Officer (OCIO)
Statement of Actions Planned to Address Office of Inspector General Draft Evaluation
Report - Information Technology Security Weaknesses at the U.S. Department of the
Interior's Core Data Center Could Expose Sensitive Data
Draft Report No. 2016-ITA-021

We recommend that BIA:

Recommendation 1: Establish an ongoing process to ensure the inventory of its systems is continually updated and accurate.

Response: Indian Affairs concurs with this recommendation and will document a process to ensure that the inventory of its systems is continually updated and accurate. It should be noted that DOI's Continuous Diagnostics and Mitigation (CDM) Phase 1 is still being implemented and upon reaching steady-state operations will incorporate CDM capabilities and processes to ensure the inventory of its systems is continually updated and accurate. DOI and DHS will complete CDM Phase 1 tools implementation later in 2017 and achieve steady-state operations between 2018 and 2019. Implementation timeframes are driven by the DHS-DOI partnership. While the implementation is funded, the sustaining operations and maintenance (O&M) resources are not programmed for 2018 and out years. Steady-state is an O&M state which follows successful implementation that can demonstrate operational effectiveness and efficiency. Indian Affairs will rely upon a combination of CDM tools as one single tool cannot satisfy the entirety of this recommendation. Timeframes for initial implementation of tools are dependent upon DHS and its contractor.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2018

Recommendation 2: Install IBM BigFix agents on all applicable BIA and BIE devices.

Response: Indian Affairs concurs with this recommendation. As of December 7, 2016 IBM BigFix was installed on 7,340 assets (96%) on the BIE network and on 5,661 assets (99%) on the BIA network. Efforts continue to install BigFix on all applicable devices and upon reaching steady-state operations will be able to demonstrate ongoing compliance with this requirement. However, Indian Affairs will rely upon a combination of CDM tools as BigFix alone cannot be used to inventory all Information Technology (IT) hardware.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2018

Recommendation 3: Implement controls that identify and remove unauthorized and unsupported products from BIA and BIE systems.

Response: Indian Affairs concurs that the implementation of controls that identify and remove unauthorized and unsupported products from BIA and BIE systems is needed in order to reach an optimized security state. CDM Phase 1 is still being implemented and upon reaching steady-state operations will incorporate capabilities and processes for software asset management controls. Specifically, Indian Affairs will use CDM Phase 1 capabilities to (a.) maintain an accurate inventory of installed software and (b.) recognize and report unauthorized software and unsupported products~ Further, Indian Affairs will work with the DOI OCIO to ensure implementation of effective (c.) procedures for removal of unauthorized products and (d.) planning support for moving away from unsupported products. Indian Affairs will rely upon a combination of CDM tools since one single tool cannot satisfy the entirety of this recommendation. Time frames for initial implementation of tools are dependent upon DHS and its contractor. The processes and procedures will be developed after the implementation of tools. Further, Indian Affairs will need this longer timeframe, which is 2019, to de-conflict software inventories while maintaining continuity of services.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2019

Recommendation 4: Ensure that critical and high risk vulnerabilities on BIA and BIE systems are mitigated within 30 days of detection in accordance with DOI policy.

Response: Indian Affairs concurs with this recommendation. As of December 15, 2016, OCIO reported that BIA had 1.23 vulnerabilities per device which placed BIA as the third best bureau/office within the entire Department in terms of vulnerability management. OCIO reported that BIE had 2.07 vulnerabilities per device. CDM Phase 1 is still being implemented and upon reaching steady-state operations, Indian Affairs will incorporate CDM capabilities and processes for vulnerability management. Specifically, Indian Affairs will use CDM Phase 1 capabilities to perform patch deployment in accordance with the NIST SP 800-40 Revision 3, *Guide to Enterprise Patch Management Technologies*, published July 2013. Indian Affairs will rely upon a combination of CDM tools as one single tool cannot satisfy the entirety of this recommendation. Indian Affairs understands that the DOI OCIO will replace the current scanning solution with a new enterprise tool. The processes and procedures will be developed after the implementation of tools.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2018

Recommendation 5: Review contracts for BIA and BIE systems managed by contractors to ensure the contract contains the appropriate Federal computer security requirements, including critical IT security controls such as vulnerability detection and mitigation.

Response: Indian Affairs reviewed the current Statement of Work for and determined that the overarching security requirements are included; however, a guidance document was produced (Contractor Information Technology (IT) Security and Privacy Requirements) to reset expectations with the contractor regarding security and privacy controls as well as to more clearly define the deliverables and reporting requirements that support those controls. This document will be shared with other BIA and BIE Contracting Officers for use in support of future Indian Affairs services contracts. Indian Affairs considers this recommendation resolved and implemented.

Recommendation 6: Monitor contractors managing BIA and BIE systems to ensure all IT security requirements are met.

Response: Specific to the OIG's findings related to vulnerability scanning and patch management for IT assets, Indian Affairs began receiving monthly reports from Infinite Campus starting in July 2016. The most recent monthly scan report was received on December 7, 2016 and shows no critical or high vulnerabilities. Indian Affairs considers this recommendation resolved and implemented.

Recommendation 7: Monitor system configuration settings to ensure BIA and BIE systems remain securely configured over time.

Response: CDM Phase 1 is still being implemented. Upon reaching steady-state operations, Indian Affairs will incorporate capabilities and processes to monitor computer operating system configuration settings to ensure computers remain securely configured. Indian Affairs will rely upon a combination of CDM tools as one single tool cannot satisfy the entirety of this recommendation. Timeframes for initial implementation of tools are dependent upon DHS and its contractor. The processes and procedures will be developed after the complete implementation of tools.

Responsible Official & Title: Thomas Hoyler, Associate Chief Information Security Officer

Target Completion Date: June 30, 2018

We recommend that OCIO:

Recommendation 8: Establish an independent verification and validation function to ensure that all Federal and Department IT security requirements are met and its data centers and the information systems they house are adequately secured.

Response: The Department's Office of the Chief Information Officer, (OCIO) concurs with this recommendation. The Compliance and Audit Management (CAM) Branch is the OCIO's independent verification and validation (IV&V) for the closure of IT audit recommendations as part of the A-50 Audit Follow-up. As part of ensuring that all Federal and Department IT security requirements are met and its data centers and the information systems they house are adequately secured, CAM conducts FISMA compliance reviews using independent auditors, and other assessments across all bureaus and offices within Interior. Similar to recommendations made in OIG and GAO IT-related final audit reports, results from these reviews and assessments are used to justify and implement improvements in the Department's IT security program. Further, OCIO has filled critical CAM leadership positions in 2016 to improve effectiveness and efficiency of its mission and functions.

Responsible Official & Title: Richard Westmark, DOI OCIO PPMD/Compliance/Audit Management Branch Chief

Target Completion Date: Complete

Appendix 3: Status of Recommendations

In its response to our draft report, the Office of the Chief Information Officer and the Bureau of Indian Affairs concurred with all eight recommendations (see Appendix 2). Based on the response, we consider seven recommendations resolved but not yet implemented and one recommendation resolved and implemented.

Recommendations	Status	Action Required
I, 2, 3, 4, 6, 7, and 8	Resolved but not yet implemented.	We will refer these recommendations to the Office of Policy, Management and Budget to track implementation.
5	Resolved and implemented.	No further response to OIG is required.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doioig.gov

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



INTERIOR INCIDENT RESPONSE PROGRAM CALLS FOR IMPROVEMENT

This is a revised version of the report prepared for public release.

Report No.: 2016-ITA-020 March 2018



MAR 1 2 2018 Memorandum

To:

Sylvia Burns

Chief Information Officer

From:

Mary L. Kendall Water Hendall
Deputy Inspector General

Subject:

Final Evaluation Report – Interior Incident Response Program Calls for

Improvement

Report No. 2016-ITA-020

This memorandum transmits the findings of our evaluation of the U.S. Department of the Interior's incident response program. We found that the Office of the Chief Information Officer had not fully implemented the capabilities recommended by National Institute for Standards and Technology (NIST) in its incident detection and response program. We make 23 recommendations to help the Department improve its incident response program, so it can promptly detect and fully contain cyber threats to maintain the availability, confidentiality, and integrity of Department and bureau computer systems and data.

In response to our draft report, the Department concurred with all recommendations and provided target dates and officials responsible for implementation. We consider all 23 recommendations resolved but not implemented. We will forward the recommendations to the Office of Policy, Management and Budget for tracking and implementation.

We understand that some of these recommendations may require significant investment in cyber security infrastructure as well as the recruitment of additional staff, but the intended timeframe to implement these recommendations remains a concern. Five recommendations will not be addressed for more than 5 years, and four recommendations will not be addressed for more than 3 years. In the interim, the Department should consider additional temporary or partial solutions.

If you have any questions regarding this report, please contact me at 202-208-5745.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

Table of Contents

Results in Brief	1
Introduction	3
Objective	3
Background	3
Incident Response Lifecycle	4
History of the Department's Network and Security	5
Findings	7
Department Not Fully Prepared to Respond to Incidents	7
Program Design Impedes Enterprise Response Capabilities	8
Slow Development of a Comprehensive Incident Response Plan	10
Inconsistent Incident Response Capabilities Across the Department	10
Department Not Capable of Consistently Detecting and Analyzing Threats.	13
No Visibility of the Department's Entire Enterprise	14
Dangerous User Behavior and Potential Threats Not Addressed	16
Testing Unnoticed by the Department	18
Risks Not Contained or Eradicated	20
Sensitive Data Can Be Exfiltrated Without Detection	21
Containment and Eradication Was Slow or Did Not Occur	22
Firewall Rules Do Not Comply With Basic Security Principles	24
Department Not Learning From Prior Incidents	25
Incident Tracking Data Not Designed to Support Post-Incident Analysis	26
Post-Incident Analysis Not Performed	28
No Enterprise-Level Oversight of Incident Analysis, Resolution, and Documentation.	28
Conclusion and Recommendations	
Conclusion	
Recommendations Summary	
Appendix 1: Scope and Methodology	
Scope Scope and Wethodology	34

Methodology	34
Appendix 2: Technical Testing Details	36
Data Exfiltration Simulation	36
Malware Simulation	36
Malicious Actor Simulation	37
Appendix 3: Response to Draft Report	38
Appendix 4: Status of Recommendations	49

Results in Brief

The U.S. Department of the Interior is a regular target of cyber attacks, both because of the large size of its computer networks, and because those networks contain technical and other sensitive information highly sought after by criminals and foreign intelligence services. We evaluated the Department's Office of the Chief Information Officer (OCIO) to determine whether it effectively follows the incident response lifecycle, as defined by the National Institute of Standards and Technology (NIST).

NIST guidance organizes the areas of an effective incident response program into four lifecycle phases: 1) Preparation; 2) Detection and Analysis; 3) Containment Eradication and Recovery; and 4) Post-Incident Activity. These phases are cyclical, continuously feeding results and performance strengths across the incident response lifecycle.

We found that the OCIO had not fully implemented the capabilities recommended by NIST in its incident detection and response program. The OCIO did not establish the foundation necessary for a mature incident response program—it did not determine objectives, define responsibilities, or manage the incident response program from an enterprise level. Without this foundation, the Department is unable to consistently perform incident response activities. Specifically, we found that the Department:

- Was not fully prepared to respond to incidents
- Did not promptly detect or fully analyze security incidents
- Did not fully contain or completely eradicate active cyber threats
- Did not continuously improve its incident response capabilities by learning from prior incidents

These issues occurred because the Department incident response program had not evolved to address today's often sophisticated cyber threats. For example, OCIO's incident response program followed an outdated model favoring the immediate remediation of a malware-infected computer and its prompt return to service over the current recommended model involving cyber threat analysis, assessment, and containment. As such, we found that the Department's approach to incident response and its focus on service delivery prevented incident responders from determining the extent of security incidents. Using a process that does not fully analyze and completely contain active cyber threats increases the risk that bureaus' sensitive data will be lost and mission operations disrupted.

Without a centralized program, Department and bureau incident response teams did not have an effective roadmap outlining policies, procedures, and responsibilities for handling incident response activities. We make 23 recommendations to help the Department improve its incident response program, so it can promptly detect and fully contain cyber threats to maintain the availability, confidentiality, and integrity of bureau computer systems and data.

Introduction

Objective

Our objective was to determine if the U.S. Department of the Interior effectively follows the incident response lifecycle, as defined by the National Institute of Standards and Technology (NIST).

In order to evaluate the Department's incident response program, we reviewed Department and bureau guidance for key elements recommended by NIST, as well as best practices. We conducted our fieldwork from March 2016 to June 2017. We interviewed staff responsible for incident response activities at selected bureaus and the Office of the Chief Information Officer (OCIO), and submitted a data call to all bureaus requesting specific capabilities and procedures. We analyzed prior incident response activities, using information available in the Department's official incident tracking system. Finally, we performed technical testing to simulate active internal threats to validate the Department's detection capabilities and response processes. See Appendix 1 for additional information on our scope and methodology and see Appendix 2 for details on our technical testing.

Background

The Department of the Interior protects and manages the Nation's natural resources and cultural heritage with nine technical bureaus and several offices. The Department accomplishes its diverse mission from more than 2,400 operating locations. These various locations and systems present a challenge to the Department in establishing and maintaining consistent security programs.

The Department is a regular target of cyber attacks both because of the large size of its computer networks and because those networks contain technical and other sensitive information highly sought after by criminals and foreign intelligence services. As such, the Department's incident response program should promptly detect and fully contain cyber threats to maintain the availability, confidentiality, and integrity of bureau computer systems and data.

The Federal Information Security Modernization Act (FISMA) requires that Federal agencies establish incident response capabilities for all systems that process, store, or transmit Federal data. Under Public Law 107-347, Section 303, NIST has the authority to develop standards and guidelines—including minimum requirements—for securing Federal information systems.

The Department's incident response capability was put to the test when a security incident occurred at a U.S. Department of the Interior data center. In October 2014, attackers moved through the U.S. Office of Personnel Management (OPM) environment through a trusted connection to the Department's data center, pivoting to human resources systems hosted by the Department. This incident was

not detected until April 2015. In today's cyber threat landscape, security incidents that result in the loss of sensitive data and disruption of business operations occur on a daily basis. As such, the Department must be able to detect and respond to security incidents to protect sensitive data and maintain business operations.

Incident Response Lifecycle

NIST released Special Publication 800-61 Revision 2 (NIST SP 800-61r2) *Computer Security Incident Handling Guide*, in August 2012. This guidance was designed to assist agencies in establishing Incident Response programs that enable them to prepare for and respond to security incidents.

NIST SP 800-61r2 organizes the areas of an effective incident response program into four lifecycle phases:

- Preparation involves limiting the number of incidents that may occur by using risk assessments in order to select and implement controls.
- Detection and Analysis detecting and analyzing security breaches is necessary for alerting agencies when incidents occur, and evaluating the type, extent, and magnitude of the breach.
- Containment, Eradication, and Recovery mitigating the impact of an incident by containing it and recovering from it. Activity in this phase often goes back to detection and analysis.
- Post-Incident Activity conducting lessons learned activities and issuing a report detailing the cause and cost of the incident and the steps to be taken to prevent future incidents.

As shown in Figure 1 below, these phases are cyclical, continuously feeding results and performance strengths across the lifecycle.

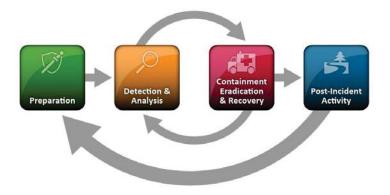


Figure 1. The NIST incident response lifecycle, as defined by NIST SP 800-61r2. Source: NIST

The incident response lifecycle also supports threat hunting activities in all phases. Threat hunting is an active, human driven activity focused on the identification of threats on the network that automated tools often fail to detect. Information generated by or documented in each phase is critical for threat hunters to have a complete view of the network environment's risks and threats.

In addition, NIST released guidance on recommended security controls in the form of Special Publication 800-53 Revision 4 (NIST SP 800-53r4) *Security and Privacy Controls for Federal Information Systems and Organizations*. This guidance was designed to assist agencies and system owners in selecting and implementing controls to improve all aspects of cyber security, including incident response planning, handling, monitoring, and testing.

History of the Department's Network and Security

The OCIO operates a large network with over 170,000 IT assets. Such large networks can provide a wide attack surface for malicious actors, if not properly designed. As such, the Chief Information Officer (CIO) delegates security responsibilities among its staff of information security professionals (see Figure 2).

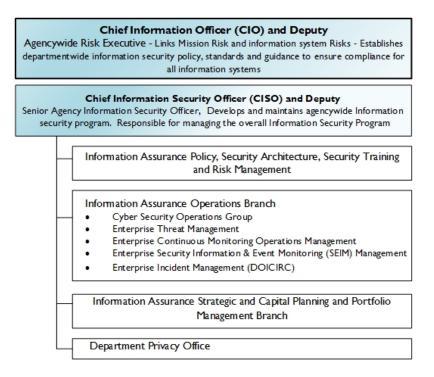


Figure 2. Security responsibilities within the OCIO. Source: OCIO

The OCIO's Information Assurance Operations Branch contains the Cyber Security Group and the Computer Incident Response Capability (DOICIRC) to provide a single IT security incident handling capability. The Information Assurance Operations Branch's roles and responsibilities states that the DOICIRC incident handlers coordinate response efforts when a critical breach, severe attack,

or computer compromise occurs. They also send e-mail alerts to the OCIO, bureau, and office incident response staff describing emerging threats. This unit reports to the Chief Information Security Officer (CISO) and the CIO.

The Cyber Security Operations Group was established in the OCIO to enhance prevention and provide early detection of security incidents, and coordinate agency-level information related to the Department's IT security posture. The OCIO developed a handbook for security incidents, and an official incident response tracking system for coordinating, tracking, and reporting incidents. As part of the Enterprise Services Network (ESN) contract, to manage security and network services, Verizon provides technical capabilities and staff resources to the Department's incident response program.

The Cyber Security Operations Group and Verizon operate incident response tools located at five Trusted Internet Connections (TICs) for the Department. The purpose of the TIC initiative is to improve and standardize security controls across individual external network connections currently in use by Federal agencies, including connections to the Internet.¹

In the recent past, the OCIO desegregated the bureaus' networks to improve service delivery, resulting in the widespread removal of internal security segmentation and monitoring programs, such as firewalls and intrusion detection systems. This focus on improving service delivery across bureau and facility boundaries came with the consequence of weakened security. This significantly increased risk to the Department's IT assets by making it easier to access these systems without security monitoring. A network without security segmentation is commonly referred to as a flat network.

¹ OMB Memorandum M-08-05, "Implementation of Trusted Internet Connections (TIC)"

Findings

We found that the Department's incident detection and response program did not effectively follow the incident response lifecycle, as defined by NIST. Specifically, we found that the Department:

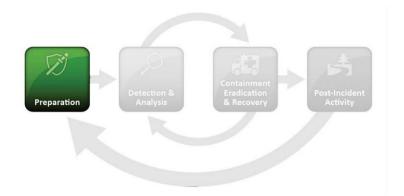
- Was not fully prepared to respond to incidents
- Did not promptly detect or fully analyze security incidents
- Did not fully contain or completely eradicate active cyber threats
- Did not continuously improve its incident response capabilities by learning from prior incidents

The OCIO did not establish the foundation necessary for a mature incident response program—it did not determine objectives, clearly define responsibilities, or manage the incident response program from an enterprise level. As such, OCIO's incident response program was not capable of detecting some of the most basic threats from inside the enterprise network. Without detecting these threats, the OCIO could not contain them in a timely manner, which left compromised systems on the network for months at a time.

These issues occurred because the Department's incident response program has not evolved to address today's often sophisticated cyber threats. For example, OCIO's incident response program followed an outdated model favoring the immediate remediation of a malware-infected computer and its prompt return to service over the recommended model of cyber threat analysis, assessment, and containment. As such, we found that the Department's approach to incident response and its focus on service delivery prevented incident responders from determining the extent of security incidents. Using a process that does not fully analyze and completely contain active cyber threats increases the risk that bureaus' sensitive data will be lost, and mission operations disrupted.

Department Not Fully Prepared to Respond to Incidents

The first phase of the NIST incident response lifecycle focuses on preparation. This phase includes the development of an incident response program as well as implementing measures to help prevent incidents from occurring.



We found that the Department's incident response program was not centralized, and the OCIO neither established roles and responsibilities nor disseminated guidance to the bureaus and offices. Specifically, the Department was not fully prepared to respond to incidents because:

- The design of the OCIO's incident response program did not follow NIST guidance. This adversely affected bureau incident response capabilities.
- The OCIO was slow to develop a comprehensive enterprise incident response plan.
- Incident response capabilities varied widely among the bureaus.

Program Design Impedes Enterprise Response Capabilities

We found that the OCIO did not have a fully developed incident response program because it had not established and communicated clear program roles and responsibilities to the bureaus. As a result, bureau incident response capabilities varied widely, which often resulted in active cyber threats not being fully analyzed and contained.

NIST² established primary elements for developing and documenting an incident response program, including specific recommendations for agencies to use when developing guidance for these programs. These primary elements include policies to define and structure an incident response program, such as defined roles and responsibilities, levels of authority, prioritization of incidents, and performance measures.

During our review, we did not find the NIST-defined elements for incident response in the Department's IT security policies. Our review found that the OCIO simply copied the NIST SP 800-53r4 Incident Response Controls section into its *Incident Response Security Control Standards*. The OCIO did not expand

-

² NIST SP 800-61r2, Section 2.3.1, "Policy Elements."

on the NIST-defined element to establish a Department policy that could be fully implemented and executed.

NIST³ also recommends additional elements to assist in planning coordinated response activities, including metrics for measuring response capabilities and effectiveness, response teams and communications, and expected strategies. We found that these additional elements were also missing from the Department's policies and procedures.

Since 2015, annual FISMA reports have indicated management control deficiencies, areas of weakness, and missing disciplines throughout the Department related to incident response. In the OIG's 2016 FISMA audit report, an independent audit team described the Department's incident response program as an ad-hoc process, or at the lowest process maturity level, because it did not have adequate documentation and dissemination of authority, responsibilities, and expectations. On October 31, 2017, the OIG FISMA audit upgraded the maturity level of the Department's incident response program from "ad-hoc" to "defined." The report noted the release of an incident response plan on August 28, 2017, and also stated that the Department's "incident response program is not effective."

In addition, we found that the OCIO had not developed an incident response team structure beyond OCIO staff. While the OCIO implemented incident detection and containment controls at the Department's five internet connections, all other responsibilities had been left to bureaus and offices with no central point of coordination. Without a centralized program, it is more difficult for bureaus and offices to coordinate and communicate with other bureaus and the OCIO.

For example, the OCIO's Cyber Security Operations Chief stated that his team was not privy to the Department's High-Value IT Asset list developed by OCIO due to its sensitive nature. High-value IT assets refer to those IT systems, facilities, and data that are of particular interest to nation-state adversaries, such as foreign military and intelligence services. Specifically, high-value IT assets often contain sensitive data or support mission-critical Federal operations. The loss or disruption of a Department high-value IT asset may be expected to have a severe adverse effect on agency operations, assets, or individuals.

Since this list was not available to those responsible for monitoring and securing the Department's most important IT resources, incident response teams could not focus their resources where they were most needed.

³ NIST SP 800-61r2, Section 2.3.2, "Plan Elements."

⁴ Independent auditors' performance audit report on the U.S. Department of the Interior Federal Information Security Modernization Act (FISMA) for Fiscal Year 2016, March 10, 2017. https://www.doioig.gov/reports/independent-auditors-performance-audit-report-us-department-interior-federal-information

Slow Development of a Comprehensive Incident Response Plan

We found that the OCIO did not have an active incident response plan. The OCIO started drafting a plan in April 2015, but did not publish it until August 2017. Some basic incident response procedures were defined in the *Interior Computer Security Incident Response Handbook* (IR Handbook), but this document did not meet the standards of an incident response plan and had not been reviewed or updated every 2 years, as recommended by NIST.

The IR Handbook did not define bureau roles within the incident response program, which has led to inconsistent development of bureau-specific incident response plans. For example:

- BSEE used obsolete Department policy as templates for developing internal incident response plans and procedures.
- The USGS incorrectly referred to OCIO's IR Handbook as an enterprise-level policy, but it was actually an incomplete set of procedures.

Without a Department-level incident response plan, the OCIO cannot ensure that bureaus and offices are properly prepared to respond to incidents in accordance with OCIO's expectations. For example, during an incident at the USGS, incident responders did not adequately preserve forensic evidence for analysis, as OCIO expected. Specifically, we identified anomalous network traffic that was not generated by our tests. The USGS team quickly found a compromised workstation, removed it from the network, and immediately began remediation activities in accordance with the USGS incident response standard operating procedure (SOP). USGS' incident response SOP prioritizes the prompt remediation of a malware-infected computer and its return to service. Based on available indicators such as foreign access attempts, our Computer Crimes Unit (CCU) began collecting data for forensic analysis, but necessary data was unavailable due to the remediation activities already performed.

The OCIO did not provide bureaus with updated guidance based on lessons learned from the 2015 OPM breach. As such, it was unaware that bureaus were still focusing on return to service priorities rather than analyzing the scope of the threat.

Inconsistent Incident Response Capabilities Across the Department

We found that bureau incident response programs evaluated and responded to cyber threats without considering the potential impact to the rest of the Department. This occurred because the OCIO had not managed the incident response program from an enterprise risk management perspective. The DOICIRC did not consistently coordinate incident response for incidents that

⁵ This was the only facility where we analyzed regular Department traffic, or traffic that we did not generate.

affected one or more bureaus. Instead, DOICIRC opened individual tickets used for incident tracking for each affected bureau. We did find that bureaus met incident handling requirements when responding to the confirmed release of personally identifiable information (PII).

With incomplete or absent departmental guidance, bureaus and offices built separate internal incident response programs with varying capabilities in terms of staff and technical resources. Figure 3, below, shows the number of dedicated incident response staff for each bureau, as well as the number of users per staff member. The two bureaus without dedicated staff each stated that incident response is not a primary duty, but considered it part of the collateral duties for existing IT security staff.

Bureau	Number of End Users	Number of Dedicated IR staff	Users per Incident Response FTE
BSEE*	2,400	7 contractors	342.8
BIA	5,800	15 contractors	386.6
BLM	10,000	3 FTE	3,333.3
FWS	13,986	0	N/A
NPS	22,890	I FTE	22,890
USBR	6,200	0	N/A
USGS	10,571	2 FTE	5,285.5

^{*} Also includes ONRR's network devices.

Figure 3. Incident response staff at each of the bureaus we reviewed, as of November 2016. Source: Bureau data call.

Interconnected systems within the Department pose risks to the enterprise, not just a single bureau or office. Without intermediary security controls using least privilege, restricting access to resources based on need, or monitoring traffic between systems, a compromised host can be used to pivot and attack other systems with a greater chance of success and a lower likelihood of detection. In order to mitigate this risk, some bureaus with available staff and funding, such as the BIA and BSEE, have implemented Intrusion Detection Systems (IDS), Network Access Control (NAC) systems, and Security Information and Event Management (SIEM) systems. These controls are intended to protect the bureau's sensitive facilities from other bureaus and offices, and further enhance controls that may not be available at the Department's internet connections. This disparity in technical resources widens the gap of capabilities and effectiveness between bureaus. Figure 4 identifies bureau-level capabilities that enhance incident response capabilities, and shows the disparity of resources between the bureaus we reviewed. Bureaus with less developed incident response capabilities are at greater risk of having undetected security threats which increases risk to the rest of the Department due to absence of network segmentation and lack of internal network monitoring.

Bureau	Bureau Specific Incident Response Technology
BSEE	NAC
BIA	NAC, IDS, IPS, SIEM,
	Malware Analysis Sandbox
BLM	SIEM
FWS	None
USBR	SIEM
ONRR	NAC
USGS	None
NPS	None

Figure 4. Bureau-level incident response capabilities, not including tools that are common throughout the Department such as firewalls, antivirus, or intrusion detection tools. Source: Bureau data call and interviews.

We found that the OCIO's enterprise incident response tools and resources were not always available to assist bureau staff when responding to incidents. As part of our evaluation, we asked all bureaus to provide the number of staff with access to the OCIO's enterprise incident response tools. We found that some bureaus had a number of staff but no access to the tools, while others had access to the tools but no dedicated staff available to use them. In addition, many bureaus were unaware of what tools were available. For example, BLM incident responders were unaware of OCIO's enterprise incident response tools, while NPS incident response tools.

When asked why access had not been provided to all bureaus, the OCIO told us that the bureaus requested to have their data be segregated by bureau to limit who could view potentially sensitive information. Many of the tools are unable to provide this level of data segregation, so those tools were not offered to the bureaus. We found, however, that at least one bureau had access to tools containing other bureaus' data—further illustrating the inconsistent distribution of access to the OCIO's incident response tools throughout the Department.

The OCIO also stated that it planned a "virtual Advanced Security Operations Center" (vASOC) capability that would expand bureau access to the OCIO's enterprise incident response tools that previously required physical access, but has been unable to implement it. The vASOC was intended to provide a unified interface for all bureau and office incident responders to view data generated by the OCIO enterprise incident response tools. The OCIO began the vASOC project in 2013, but the hardware to support it was loaned to a different program in 2014. As of October 2017, the hardware required to implement the vASOC had not been returned to the Cyber Security Operations Group. Further, additional funding was

not provided to purchase replacement equipment. The OCIO continues to pursue this capability, but has not acquired the resources to implement it.

Recommendations

We recommend that the Department:

- I. Create comprehensive policy, as described by NIST guidance, for the incident response security program that prescribes:
 - Organizational priorities
 - · Roles, responsibilities, and levels of authority
 - Performance measures
 - Reporting requirements
- 2. Utilize the Department's High-Value IT Asset list to develop prioritized event monitoring and incident response activities.
- 3. Develop a Department-level incident response plan and procedures that incorporate:
 - Strategies and goals, to include metrics for measuring effectiveness
 - Incident response team structure
 - Communication plans
- 4. Review bureau-specific incident response plans and procedures to ensure alignment with the Department's incident response plan.
- 5. Develop a solution for providing bureaus consistent access to the enterprise incident response tools, and provide additional event analysis in the interim.

Department Not Capable of Consistently Detecting and Analyzing Threats

The second phase of the incident response lifecycle focuses on detecting and analyzing potential and active threats. The faster a threat (e.g., a computer virus) can be recognized the quicker it can be mitigated. Early threat recognition can minimize the effect of an ongoing incident or prevent one altogether.



In order to evaluate OCIO's detection and analysis capabilities, we performed technical testing at several bureaus and locations within the Department's network. We found that the OCIO:

- Did not have visibility into the Department's entire enterprise infrastructure
- Chose not to address potential threats and dangerous user behavior
- Did not detect most of the security incidents produced from our testing including the simulated exfiltration of sensitive data

These issues occurred because the OCIO divided the responsibility for detection and analysis at an organizational level. The OCIO and several bureaus have the capabilities to share incident data across the enterprise to coordinate incident response, but incident response teams often did not have the authority or ability to analyze events across the enterprise. Operating independently without effective coordination between teams has left the Department and its bureaus unaware of—and vulnerable to—active threats within the enterprise.

Further, the OCIO did not have a team actively engaged in threat hunting—the active, human-driven search for anomalous events by dedicated, experienced team members. Each incident response team was limited to bureau priorities, focusing activities on alerts generated by tools.

No Visibility of the Department's Entire Enterprise

We found that the OCIO did not have an enterprise-wide view of incidents occurring within its network. The OCIO did not have visibility of bureau- and office-level incidents or event data. Further, OCIO did not have a single mechanism for tracking and evaluating data as incidents occur or after they have been resolved.

The OCIO was not able to correlate the event data from all OCIO and bureau systems that was generated by our tests, which simulated the exfiltration of sensitive data, compromised machines, and active malicious threats. By

aggregating this data and analyzing as a whole, incident responders would have been able to more quickly identify our behavior as a potential threat. To determine if OCIO staff could detect or prevent our activity, we analyzed data from the OCIO's enterprise incident response tools. We requested data from the OCIO's incident responders to determine if there was a human response to our activity, and we also used our own tools to monitor our testing activity. We found that event data was segregated across multiple systems that were separately operated and funded—making it nearly impossible to automatically correlate and analyze anomalies across the enterprise. This practice increased costs because some systems had duplicate functionality and agents, while the human element was still missing.

The OCIO's ability to correlate incident information across the enterprise was limited. USGS maintains an official incident tracking system for all bureaus and offices for the OCIO. Most bureaus, however, hosted their own internal incident tracking systems, and only informed the OCIO of incidents that met a bureau-determined threshold. This threshold was usually a bureau's interpretation of the mandatory US-CERT⁷ (U.S. Computer Emergency Readiness Team) reporting after the confirmed loss of PII. This left the OCIO unaware of incidents that may have been crossing organizational boundaries, and minimized opportunities for the OCIO to provide advanced warnings to bureaus not yet affected.

NIST SP 800-53r4 recommends practices for manual and automated audit log practices. Audit logs must be retained for adequate support of after-the-fact investigation of security incidents. Enterprise threat detection via event correlation is typically accomplished with a Security Information and Event Manager (SIEM) and a group of knowledgeable and engaged responders. A SIEM provides real-time correlation and analysis of logged events generated by any device on the network from which it receives data. The OCIO, bureaus, and Verizon worked independently to implement separate SIEM solutions—these standalone systems did not share or collect data from each other.

In its DOI Cybersecurity Strategic Plan for fiscal year 2016, the OCIO documented the need for an enterprise SIEM for incident response, but it was not a funded priority. The Cyber Security Operations Group has begun testing a log aggregation tool that will collect log data from multiple OCIO systems. The OCIO plans to feed this data directly into an enterprise SIEM solution in the future. We noted the following disparate SIEM installations:

 Event logs from departmental VPN servers were sent to a SIEM operated by Verizon.

⁶ We did not have access to all of the OCIO's enterprise incident response tools.

⁷ https://www.us-cert.gov/about-us

- Event logs from Active Directory were sent to a SIEM operated by the OCIO.
- Event logs from bureau-operated systems were correlated in multiple disparate SIEM operated by individual bureaus.

As a result, some bureaus acquired and implemented their own SIEM solutions. In addition, the U.S. Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program includes plans and funding for implementing a SIEM.

In addition, we found that the OCIO did not engage in active threat-hunting activities, searching for potential threats across organizational boundaries within the Department. The OCIO's enterprise cyber security operations teams had not been assigned the responsibility to track down incidents that pose a risk to the entire Department. Threat-hunting teams require experienced cybersecurity personnel with backgrounds in multiple information technology fields, such as digital forensics, networking, system administration, and security. Instead of building a threat hunting team, OCIO relied on automated alerts. Automated alerts can only detect anomalies based on pre-determined signatures and are often filled with minimal relevant data. Automated threat detection systems not properly tuned for their environment typically have a large number of false positives and negatives. The Department was missing the human interaction when analyzing alerts, events, and active processes across the environment necessary to find well-hidden intruders and tune systems to capture the most relevant event data.

In addition, the OCIO did not consolidate enterprise tools that could share event management servers. For example, each bureau operated a separate antivirus system that logged to separate management servers within each bureau, while using the same product.

Dangerous User Behavior and Potential Threats Not Addressed

We found that the OCIO's incident response teams did not always notify their bureau counterparts of security alerts, which may indicate that a bureau computer may be compromised. Some of these alerts were generated when a bureau user engaged in inappropriate conduct, such as browsing a website hosting pornography or one that streamed pirated videos. This occurred because the OCIO considered end-user behavior policy and enforcement to be a bureau-level responsibility. A policy that does not include inappropriate usage as a potential cyber threat can adversely affect information security. Websites containing pornographic and pirated material often host malicious software. Frequenting such websites may result in malware infections which, if unaddressed, can quickly spread throughout an organization.

Moreover, computer network traffic originating from a bureau computer, which was blocked because it was headed to a known malware command and control

site, can also be a potential indicator that the computer is compromised. According to the OCIO, its standard practice was not to notify bureaus of this potentially malicious traffic.

During our technical testing at a USGS facility, we discovered suspicious traffic originating from a user workstation. Our device, which was monitoring USGS network traffic, identified a USGS workstation attempting to communicate with IP addresses of known malware command and control websites in Russia. After we alerted the bureau team of the anomalous traffic, they discovered that the machine in question had been compromised.

We assisted the team with network forensics and reviewed the machine's network activities based on data recorded by the TIC security devices. A review of network traffic showed that the user had been frequenting websites that hosted pornography. The CCU later confirmed that the user had been downloading pornographic material and saving it to an external drive. This behavior triggered security alerts that were logged by OCIO-level incident response tools, but not by the USGS incident response tools. Moreover, the OCIO incident responders failed to notify their USGS counterparts of this potential security incident on the USGS network. We also discovered machines on the USGS network that were actively streaming pirated media from Russian and Ukrainian websites.

As another indicator of compromise, event logs from internal facility network devices showed that a machine was regularly transmitting NetBIOS⁸ lookup requests to computers in Russia. The NetBIOS traffic was blocked before leaving the network, but the USGS facility staff did not analyze the alerts. Since the USGS network security devices blocked the NetBIOS traffic, it was never seen by OCIO incident response tools. CCU later found that this machine had also been infected with malware.

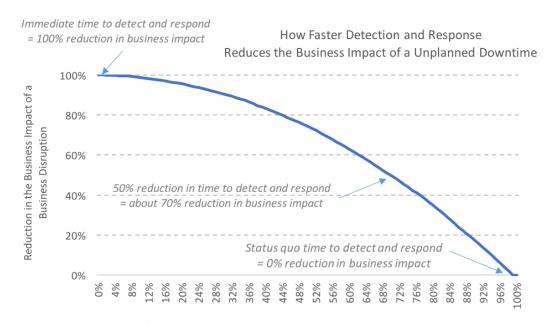
Our discussions with the USGS and OCIO's Cyber Security Operations staff revealed that blocked potential threats and dangerous or inappropriate user behavior were not investigated. Instead, the OCIO's Cyber Security Operations Group had been instructed to focus on widespread or confirmed incidents.

Industry data shows that the impact of a security breach is directly proportionate to the amount of time taken to detect and respond to that breach (see Figure 5). OCIO's blocking of anomalous traffic from bureau computer networks without alerting the affected bureau of the potential cyber threat can result in threats going undetected. Undetected threats increase the risk of losing sensitive data or a

⁹ Cybersecurity: For Defenders, It's About Time, Aberdeen Group report commissioned by McAfee based on data provided by Verizon, dated April 2017.

⁸ NetBIOS is an acronym for Network Basic Input/Output System and is used for allowing computers to communicate over a local area network. NetBIOS traffic that attempts to exit an organization's network is a common indicator of malicious activity.

disruption to bureau operations. This directly led to multiple compromised machines remaining on the Department's network for an indeterminate amount of time.



Time for Threat Detection and Incident Response, Relative to the Status Quo

Figure 5. Analysis performed by Aberdeen Group shows that faster detection and response reduces the business impact of a data breach. Source: *Cybersecurity: For Defenders, It's About Time*, Aberdeen Group report commissioned by McAfee based on data provided by Verizon, dated April 2017.

After completing our technical testing, we returned to the USGS facility to work with local information security staff to validate the extent of the previously identified threats, and to assist with developing internal threat-hunting techniques. The USGS facility staff have since added active threat hunting to the regular duties of the local information security staff, which we consider a best practice.

Testing Unnoticed by the Department

While OCIO's enterprise incident response tools detected many of our tests, most of the alerts went unnoticed by OCIO staff. This occurred because OCIO incident response staff did not analyze alerts generated by all tools.

Over a 4-week period, we tested the Department's incident response capabilities by simulating active cyber threats on bureau computer networks. One of our tests, though benign, generated hundreds of thousands of security alerts that were recorded by an OCIO enterprise incident response tool. We found, however, that OCIO incident response staff did not review or respond to these alerts until 2 weeks later, March 20, 2017, when a different tool alerted incident response staff of a potential security incident. Although the second tool is more heavily relied on, it was slower to recognize our activity, and generated less than 20 alerts for

the same test. When we asked for a summary of their response activities, the OCIO staff described the alerts from the first tool as not significant enough to warrant additional research, and also noted that blocked events do not normally trigger human activity. Once these tests were finally recognized as a threat by the second tool, the OCIO took actions to contain them.

OCIO incident response staff also did not react to any of our other tests until US-CERT identified and alerted the Department of a potential insider threat. ¹⁰ We began performing multiple ransomware file transfers on February 27, 2017. On March 22, 2017 US-CERT identified our activity as a potential insider threat. US-CERT then analyzed our activity and notified the Department of the potential threat on March 28, 2017.

We found that multiple OCIO tools began recognizing our tests on March 22, 2017. Due to a misunderstanding of the various alerts generated, the OCIO mistakenly concluded that all activity was blocked when in fact, several of the tests successfully downloaded ransomware. The OCIO's first incident response ticket for our ransomware tests was created on March 28, 2017—more than a month after our testing began.

¹⁰ US-CERT Amber Alert, reference no. INAR-17-000008

Recommendations

We recommend that the Department:

- 6. Identify areas of high risk on the Enterprise Services Network (ESN), (e.g. data centers, science centers, DMZ networks) and extend enterprise incident response tool visibility to those areas.
- 7. Require all security incidents be tracked in a single enterprise system that allows Departmentwide incident correlation.
- Accelerate plans to implement a Security Incident and Event Manager (SIEM)
 that can analyze and correlate events across multiple, disparate systems that
 incorporates data feeds from all security tools and infrastructure systems, to
 include those managed by the bureaus or third-party contractors.
- Evaluate security tools with overlapping capabilities, such as antivirus and firewalls, for consolidation to reduce the number of disparate log management and alerting systems.
- Define and enforce minimum Departmentwide standards on log collection and retention that are sufficient for performing event and security incident analysis.
- 11. Develop a dedicated group of incident responders to perform threat hunting and containment activities with:
 - Advanced analytical experience across multiple disciplines
 - Authority to access Departmentwide event data
 - Authority to engage organizationally segregated IT staff
- 12. Develop a Departmentwide methodology to address inappropriate and prohibited internet usage, to include departmental monitoring and a risk analysis of events.

Risks Not Contained or Eradicated

The third phase of the incident response lifecycle, containment, eradication, and recovery, is key to responding to an incident. After the foundation has been established to prepare for an incident, informed decisions can be made on how best to respond when an incident occurs. Fast detection of threats on the network is critical to effective containment—a review of public, high-profile security incidents over the past 2 years revealed that the longer a system is compromised, the higher the risk of a disruption to operations or the loss of sensitive data.



Because our tests, which simulated actual cyber threats, often went undetected by the OCIO and bureaus, we were unable to fully measure the Department's capabilities to contain and eradicate cyber threats. As such, we found that:

- Sensitive data could be exfiltrated without detection.
- Containment and eradication was slow or did not occur.
- Firewall rules do not comply with basic security principles.

Firewall configurations and the use of publicly routable IP addresses to the desktop generated a significant amount of log events, which overloaded incident responders with too much data. As a result, it was difficult for the OCIO to determine which inbound traffic was legitimate, and which was an indicator of compromise.

Sensitive Data Can Be Exfiltrated Without Detection

During our testing, the OCIO did not detect or prevent the exfiltration of sensitive information such as PII. As part of our technical testing, we created sample Microsoft Word and Microsoft Excel documents that contained simulated PII. These documents each had 10, 100, 1,500, and 10,000 fake names, credit card numbers, and social security numbers. Each document also had a cover page that contained our project number and a request to contact us directly if recovered. We simulated data exfiltration by transferring these documents to a cloud-based system managed by our team using several methods. The OCIO did not detect any of these tests.

We found that the new web Data Loss Prevention (DLP) tool used by OCIO did not block our attempts to exfiltrate sensitive data from bureau computer networks, nor did it generate alerts containing sufficient information for incident responders to analyze our activity. To save costs, the OCIO transferred web DLP responsibilities to a tool included in its Verizon contract. We analyzed reports from both the old and new DLP tools, and found that the new web DLP tool did not have the same functionality available in the old tool, which was critical for analyzing the incident. For example, reports from the new web DLP tool did not

contain enough information to allow an incident responder to understand the extent of a potential data loss incident. The reports included the date and time, the file name, and the URL. The reports did not include information such as a copy of the transferred file which would allow responders to determine what type of PII was included, how many instances of PII were transferred, or whether the incident is a false positive.

The new web DLP tool was configured to allow all traffic and generate a log entry if PII is detected above a specific threshold. After each site test, we logged into the OCIO's web DLP tool and downloaded reports of all activity discovered by the tool. The web DLP only detected when we exfiltrated test documents with 100 or more PII entries over common network services, such as HTTP or FTP. The web DLP tool did not detect any unencrypted file transfers disguised by other network services—a popular tactic for malicious actors to hide their network traffic in plain sight.

Containment and Eradication Was Slow or Did Not Occur

We found that the OCIO was unaware of our testing to simulate a malicious actor on the network looking to burrow further into the Department's infrastructure. Working from within the Department network, we targeted servers for easily detectable reconnaissance and vulnerability scans. These servers were hosted within DMZ¹¹ networks operated by the OCIO or the bureaus. The OCIO did not respond to these tests. After testing, we noticed that some bureau-operated logs contained evidence of our tests, but this data was not visible to the OCIO and elicited no response.

In addition, we were able to hide much of our activity from the Department using encrypted remote access sessions. The OCIO did not contain encrypted outbound traffic commonly used to create remote access sessions. Intruders use these sessions to disguise their network activity from automated detection tools, remotely control compromised devices in the Department, or simply bypass controls intended to protect the Department from malicious websites and inappropriate content.

We found that the OCIO also did not detect or block the use of remote desktop sharing tools. These tools create a bridge between a computer on the Department's internal network and one connected to the internet outside the Department. Once configured, computers may be operated remotely by malicious actors or typical helpdesk support scam operations. These external bridges pose

publicly-accessible-information-technology-systems

¹¹ Demilitarized Zone (DMZ) is a technical term for an isolated network that is used to allow public access to services while protecting internal resources such as local area networks. Our evaluation report on "Security of the U.S. Department of the Interior's Publicly Accessible Information Technology Systems," Report No: ISD-IN-MOA-0004-2014 found that the Department did not properly configure its DMZ networks to protect its internal resources. https://www.doioig.gov/reports/security-us-department-interior%E2%80%99s-

additional threat entry points into the Department's network and additional data exfiltration methods.

We used three remote desktop sharing tools to connect to computers on the Department's network from computers outside the network. One of these remote access tools was not detected by Department security devices, and Department incident responders did not respond to the alerts generated by the other two. These tools can often be used for remote access by well-meaning employees, but the OCIO has an official policy, published in August 2006, requiring that all remote access connections use the OCIO-managed VPN solution. The TIC security controls had the ability to enforce this policy by containing this activity, but were not configured to do so.

We also found that the OCIO's enterprise incident response tools did not block use of The Onion Router Browser (TOR Browser). The TOR Browser is used to anonymize web-based network traffic and to access the dark web. ¹² A Verizon tool detected one of our tests using the TOR Browser, and Verizon promptly contacted DOICIRC to investigate. DOICIRC contacted the bureau via email, but did not open a ticket or document the investigation in the official tracking system. Most of our TOR Browser testing went undetected. In addition, CCU's investigation into the compromised machine at USGS found that the TOR Browser executable was present, and may have been executed.

We found that the OCIO was unable to detect and prevent common malware within a reasonable timeframe. It took 26 days for the OCIO to react to our infection simulation, because it relied more heavily on network-based IPS tools. The executable ransomware file we used for the test was identified by 45 of 58 analysis tools ¹³ prior to our testing, including Verizon's web-based antivirus. Verizon's web-based antivirus successfully blocked our transmission of the malware, but was unable to detect and block the ransomware when we hid it inside of a compressed file that exceeded 5 Megabytes (Mb). The OCIO chose not to address the alerts from the web-based antivirus because OCIO routinely does not investigate blocked events. The network-based IPS began detecting and alerting on the 5Mb file on March 23, 2017. This triggered OCIO's first acknowledgement of the alert only, erroneously believing it had been blocked, which was 26 days after we began testing. The network-based IPS did not block our 5Mb ransomware file transfers until the final day of our testing, March 30, 2017.

¹² The dark web consists of websites that are visible to the public, but whose direct locations are intentionally hidden. This supports legitimate privacy concerns, but also enables criminal activity such as gambling, illegal drug sales, and the sharing of child pornography.

¹³ To ensure we were testing with easily detectable malware, we submitted the malware sample to VirusTotal.com. VirusTotal is a website that facilitates antivirus scanning of uploaded files. At the time we uploaded the malware, VirusTotal tested it against 58 tools, and 45 of those tools successfully identified the malware.

Further, at the NPS, we discovered that audit logs were being overwritten by new events due to inadequate storage space. The NPS reported that by the time they received an alert regarding possible threats, log data was no longer available for analysis. This prevented the NPS and Department staff from identifying compromised systems. The NPS has been aware of the issue since 2008, and the identified risk was later accepted with the expectation that the OCIO would provide a Departmentwide solution. As part of a briefing in August 2017, the NPS agreed that this was no longer an acceptable risk and that it would work with the OCIO to find an interim solution in accordance with guidance within NIST SP 800-53r4.

Firewall Rules Do Not Comply With Basic Security Principles

We analyzed the Department's TIC firewall rules and found that they permitted excessive inbound and outbound traffic. This significantly reduced the OCIO's ability to contain potential incidents, as we demonstrated with our technical testing.

The *TIC Reference Architecture 2.0* establishes the minimum TIC standards required for all Federal agencies. This document states that packet filtering (e.g. firewalls) on external connections (e.g. internet) is both mandatory and required to be performed by the TIC access point. The TIC Reference Architecture 2.0 also states that firewall policies should:

- Block unsolicited inbound services by default
- Allow only approved inbound and outbound services
- Only permit approved source and destination IP addresses

When the OCIO consolidated network access under the initial TIC requirements, the USGS requested authorization to maintain its own firewalls instead of being subject to the TIC firewall rules. The OCIO agreed, and exempted USGS from the default TIC firewall rules. The additional permitted traffic caused confusion among incident responders during the compromised workstation incident at a USGS facility. We notified the USGS of this issue and it concurred that this does not meet TIC requirements, and agreed to work with the OCIO to ensure that compliant default rules will be implemented at the TIC.

We also found that excessive outbound traffic was permitted through the TIC firewalls. This occurred because of the OCIO's lax change management procedures for firewall rules. We reviewed the change management requests and justifications for all outbound traffic rules. While some change requests included narrowly defined requirements, these changes were applied Departmentwide rather than limiting the scope of these changes to the defined requirements. By not following the basic security principle of least privilege when implementing firewall rules, the risk of data exfiltration increased.

In addition, at ONRR we found a circuit connecting a Denver facility with a third-party hosting facility that bypassed the TIC architecture – including the firewalls. Traffic flowing across this circuit was not visible to the OCIO or the enterprise incident response tools. We notified ONRR of the risk this posed to the rest of the Department, including enterprise interconnected bureaus who were not aware of the connection or able to analyze and consider compensating controls. ONRR concurred with our assessment and agreed to work with the OCIO to relocate the circuit from the ONRR internal network to a TIC protected interface.

Recommendations

We recommend that the Department:

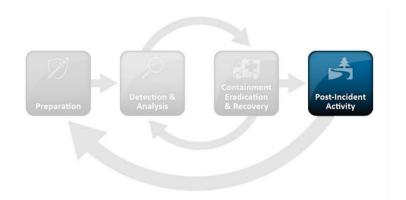
- 13. Configure all DLP systems to block the transfer of sensitive information.
- 14. Ensure all DLP systems provide sufficient data to allow incident responders to accurately identify and assess the impact of potential incidents.
- 15. Ensure DMZs are configured to log and report events to a centralized SIEM.
- 16. Define a Departmentwide baseline of inbound and outbound TIC firewall rules that incorporates:
 - Least privilege principle
 - Inbound rules to terminate at a DMZ, not internal networks
 - Periodic testing to validate that rules are operating as intended
- 17. Validate that all TIC firewall rules have a currently valid business case and a risk analysis, and remove those that do not.
- 18. Identify external connections that are not visible to enterprise incident response tools and migrate them to the TIC.

Department Not Learning From Prior Incidents

The fourth phase of the incident response lifecycle, Post-Incident Activity, helps improve an organization's incident response capability by incorporating "lessons learned" on prior incidents. According to NIST¹⁴, well-documented incident response activities using appropriate metrics are critical for learning from the past and improving for the future. Lessons-learned exercises determine the effectiveness of the incident handling process and identify necessary improvements for existing security controls and practices. Because the Department has a flattened network, this phase should be conducted from an enterprise view to reduce the risk of incidents repeating across bureau networks.

¹⁴ NIST SP 800-61 R2

The NIST guidance provides a suggested list of metrics that should be recorded, at a minimum, to successfully conduct post-incident activities. ¹⁵ Further, the NIST guidance states that lessons-learned activities should be performed using both objective and subjective metrics gathered during the incident reporting process.



We found that:

- The OCIO's official incident tracking system was not designed to support post-incident analysis.
- The OCIO did not perform post-incident analysis.
- The OCIO did not provide oversight to ensure that past incidents were analyzed, resolved, and documented.

These issues occurred because the OCIO did not monitor the official incident tracking system to ensure data being input was timely, complete or accurate because it considered these activities to be a bureau responsibility. Without proper use and quality assurance, the data within the tracking system cannot be fully analyzed to support the phases of the incident response lifecycle. Further, the OCIO's official incident tracking system was not designed in accordance with NIST guidance, and its poor design has led to inconsistent and unreliable data.

Without reliable metrics, the OCIO cannot accurately measure the efficacy of its incident response program. Management has not defined or developed incident response metrics and, as a result, the OCIO has missed opportunities for improving the Department's overall security posture.

Incident Tracking Data Not Designed to Support Post-Incident Analysis

We found that OCIO's official incident tracking system was not designed with the data elements and metrics required for performing post-incident analysis. For

¹⁵ NIST SP 800-61 R2, Section 3.4.2, "Using Collected Incident Data."

example, we could not determine the amount of time spent on different aspects of analysis, containment, and recovery for each incident. In addition, OCIO staff could not assess incidents and their resolution because indicator information, incident documentation, analysis data, or impact valuations were not always available. The system does not require that these key elements be conducted, documented, or submitted prior to closing an incident ticket.

Without appropriate metrics, OCIO cannot identify successes or opportunities for improvement. Threats are changing daily, which in turn requires response activities to continuously adapt in order to detect and mitigate malicious activity in a timely manner. Changing incident response processes and controls without appropriate measurement could have a detrimental impact on the controls already in place, as demonstrated during our technical testing.

In addition to the poor design, we found that the official incident tracking system was not being used as intended due to inadequate training and guidance. For example, each bureau interpreted the incident reporting requirements differently, resulting in inconsistent data in the system.

In addition, the OCIO's incident response team routinely documented firewall rule changes in the incident response system. This information belongs in the official change management database, where an appropriate enterprise risk analysis can be performed. As a result, future risk analyses may be based on incomplete information.

Further, existing database fields were used inappropriately, resulting in inaccurate information. For example, the OCIO's official incident tracking system had three "Incident Type" categories that do not represent types of incidents. These three incident types are labeled as "DOICIRC," "ASOC," and "US-CERT." The OCIO used these incident types to show who reported the incident, rather than the type of incident that occurred. By using the incident type field in this manner, the OCIO mischaracterized the incidents, which reduced the effectiveness of the official incident tracking system because it had no assurance of accuracy. Some system discrepancies included:

- 18 percent of analyzed tickets that were labeled incorrectly would not appear in reports generated by incident type. For example, a phishing incident labeled as "ASOC" would not appear in a report for all "phishing" incident types.
- 69 percent of analyzed tickets assigned the "DOICIRC" incident type were not incidents, and instead were operational management notes.
- 74 percent of analyzed tickets assigned the "ASOC" incident type were not incidents, and instead were firewall rule changes.

During our evaluation, we briefed the OCIO of our potential findings related to the official incident tracking system. In response, the CISO stated that the OCIO "does not need metrics to perform incident response." While metrics are not necessary to respond to a single incident, they are necessary for improving detection, analysis, containment, mitigation, and recovery for all future incidents. Having clearly defined metrics to review can help reduce delays in future detection and mitigation results.

Post-Incident Analysis Not Performed

We found that the OCIO did not conduct post-incident analysis on any of the tickets we reviewed. We selected a sample of 328 of the 3,159 tickets opened in the OCIO's official incident tracking system between January 1, 2014, and February 28, 2016, representing approximately 10 percent of all tickets opened during our selected timeframe.

Of the incidents we reviewed, only 82 percent were adequately documented for us to understand the incident and its resolution. None contained documentation of a review for lessons-learned activities by the OCIO. One ticket had documentation of additional security controls implemented by a bureau to prevent a repeat of the incident. We could not find any evidence of enterprise-level analysis for lessons learned in the official incident tracking system.

The OCIO's Cyber Security Operations teams stated that they do not have time to perform adequate incident documentation or to document lessons learned. Further, 43 of the 3,159 tickets remained open without resolution as of August 21, 2017—more than a year after being created.

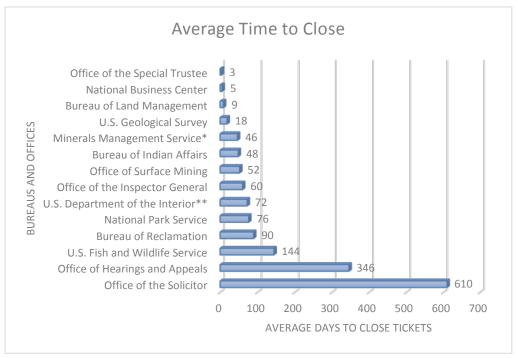
No Enterprise-Level Oversight of Incident Analysis, Resolution, and Documentation

We found that the OCIO did not monitor open incident tickets to ensure they were resolved with appropriate analysis and mitigation. Instead, the OCIO only monitored the amount of time tickets were open in the official incident tracking system.

The absence of defined incident response team roles has contributed to the misuse of the official incident tracking system. The OCIO's Cyber Security Operations Group did not think they had the authority to require bureaus and offices to use the system and did not effectively communicate expectations. Without official guidance, bureaus relied on their own interpretations of what type of information or level of detail should be documented in the official incident tracking system.

The DOICIRC staff generated monthly reports regarding the number of open incidents and forwarded this information to the bureaus, requesting that the reported tickets be closed at the bureaus' "earliest convenience." It did not appear, however, that the bureaus were responding to these reports. The OCIO did not analyze bureau updates to tickets because it did not consider bureau incident

activities to be under its purview. As a result, we found a disparity in the length of time taken to resolve incidents, as shown in Figure 6 below.



Note: The labels in this graph came directly from OCIO's official incident tracking system. Tickets maintained in bureau-level systems were not included.

Figure 6: The average number of days between incident start to resolution varies by bureau. Source: OCIO.

Most bureaus hosted their own internal incident tracking systems and only copied incident data into the OCIO's official incident tracking system if they met a bureau-determined threshold. This threshold was usually the bureau's interpretation of mandatory US-CERT reporting after the confirmed loss of PII. This left the OCIO unaware of current incidents that may have been crossing organizational boundaries, and limited opportunities for advanced warnings to bureaus not yet affected. This also limited the OCIO's ability to correlate events that may have indicated a related incident occurring elsewhere.

^{*}The BOEM, BSEE, and ONRR were still combined under the Minerals Management Service label in this system.

^{**}The U.S. Department of the Interior label represented groups or offices within the Department's purview.

Recommendations

We recommend that the Department:

- 19. Replace or redesign the official incident tracking system, as described by NIST guidance, to include:
 - All required metrics
 - All phases of the incident response lifecycle
 - Security controls applicable to all stored data types
- 20. Provide periodic training to incident response teams on the appropriate and consistent use of the incident tracking system.
- Require change control events be processed and recorded in official change control management systems instead of in the official incident tracking system.
- 22. Develop processes for periodically performing lessons-learned activities and implement program improvements where warranted.
- 23. Develop and implement a quality control program that periodically reviews tracked incidents to ensure they include documentation and analysis of the extent, impact, and mitigation activities.

Conclusion and Recommendations

Conclusion

The NIST incident response lifecycle is cyclical, continuously feeding results and performance strengths back into each phase. Since the OCIO did not establish the foundation necessary to successfully prepare for responding to incidents, the Department could not detect, contain, or recover from incidents in a timely manner. The Department did not perform post-incident analysis activities and, therefore, did not complete the feedback loop to improve its incident response program.

The Department's decentralized management and authority across the OCIO and bureaus, combined with the flattened internal networks has eliminated many of the technical boundaries within the Department's network. Malicious actors use these blind spots to hide for extended periods of time, allowing the exfiltration of sensitive information.

The bureaus and offices had varying levels of capabilities, resources, and approaches to incident response. Even those with more incident response resources relied heavily on the OCIO for perimeter security controls and monitoring services, which were inconsistently shared with the bureaus. Tools, however, are not enough. Human interaction is needed to monitor and respond to incidents, which would truly elevate the Department's incident response capabilities.

The impact of security incidents is amplified because the OCIO has accepted the risk of operating a flattened enterprise network with decentralized management controls. As such, it is imperative that the Department's incident response program promptly detect and fully contain cyber threats to maintain the availability, confidentiality, and integrity of bureau computer systems and data.

Recommendations Summary

In response to our draft report, the Department concurred with all recommendations, and provided target dates and officials responsible for implementation. The Department's full response is included in Appendix 3.

We recommend that the Department:

- 1. Create a comprehensive policy, as described by NIST guidance, for the incident response security program that prescribes:
 - Organizational priorities
 - Roles, responsibilities, and levels of authority
 - Performance measures
 - Reporting requirements

- 2. Utilize the Department's High-Value IT Asset list to develop prioritized event monitoring and incident response activities.
- 3. Develop a Department-level incident response plan and procedures incorporate:
 - Strategies and goals, to include metrics for measuring effectiveness
 - Incident response team structure
 - Communication plans
- 4. Review bureau-specific incident response plans and procedures to ensure alignment with the Department's incident response plan.
- 5. Develop a solution for providing bureaus consistent access to the enterprise incident response tools, and provide additional event analysis in the interim.
- 6. Identify areas of high risk on the Enterprise Services Network (ESN), (e.g. data centers, science centers, DMZ networks) and extend enterprise incident response tool visibility to those areas.
- 7. Require all security incidents be tracked in a single enterprise system that allows Departmentwide incident correlation.
- 8. Accelerate plans to implement a Security Incident and Event Manager (SIEM) that can analyze and correlate events across multiple, disparate systems that incorporates data feeds from all security tools and infrastructure systems, to include those managed by the bureaus or third-party contractors.
- 9. Evaluate security tools with overlapping capabilities, such as antivirus and firewalls, for consolidation to reduce the number of disparate log management and alerting systems.
- 10. Define and enforce minimum Departmentwide standards on log collection and retention that are sufficient for performing event and security incident analysis.
- 11. Develop a dedicated group of incident responders to perform threat hunting and containment activities with:
 - Advanced analytical experience across multiple disciplines
 - Authority to access Departmentwide event data
 - Authority to engage organizationally segregated IT staff
- 12. Develop a Departmentwide methodology to address inappropriate and prohibited internet usage, to include departmental monitoring and a risk analysis of events.

- 13. Configure all DLP systems to block the transfer of sensitive information.
- 14. Ensure all DLP systems provide sufficient data to allow incident responders to accurately identify and assess the impact of potential incidents.
- 15. Ensure DMZs are configured to log and report events to a centralized SIEM.
- 16. Define a Departmentwide baseline of inbound and outbound TIC firewall rules that incorporates:
 - Least privilege principle
 - Inbound rules to terminate at a DMZ, not internal networks
 - Periodic testing to validate that rules are operating as intended
- 17. Validate that all TIC firewall rules have a currently valid business case and a risk analysis, and remove those that do not.
- 18. Identify external connections that are not visible to enterprise incident response tools and migrate them to the TIC.
- 19. Replace or redesign the official incident tracking system, as described by NIST guidance, to include:
 - All required metrics
 - All phases of the incident response lifecycle
 - Security controls applicable to all stored data types
- 20. Provide periodic training to incident response teams on the appropriate and consistent use of the incident tracking system.
- 21. Require change control events be processed and recorded in official change control management systems instead of in the official incident tracking system.
- 22. Develop processes for periodically performing lessons-learned activities and implement program improvements where warranted.
- 23. Develop and implement a quality control program that periodically reviews tracked incidents to ensure they include documentation and analysis of the extent, impact, and mitigation activities.

Appendix I: Scope and Methodology

Scope

The scope of this evaluation includes enterprise incident response program and capabilities throughout the Department. We conducted our evaluation from March 2016 to June 2017. We analyzed the incidents entered into the Office of the Chief Information Officer's (OCIO's) official incident tracking system from January 1, 2014, through February 28, 2016. Our methodology for analysis varied based on the Incident Type category in the official incident tracking system.

Methodology

To accomplish our evaluation objectives, we—

- conducted interviews with subject matter experts at the OCIO, bureaus, and Verizon
- conducted a data call to the bureaus
- reviewed system security and incident response documentation for the OCIO and all bureaus
- reviewed firewall rule configurations for each of the five Trusted Internet Connection (TIC) gateways
- reviewed past security incidents
- developed scripts and network tests for technical testing
- analyzed the results of our technical tests

We selected the Department's OCIO, Verizon, and five bureaus for interviews based on their geographical locations of incident response staff:

- U.S. Fish and Wildlife Service (FWS)
- Office of Natural Resources Revenue (ONRR)
- Bureau of Land Management (BLM)
- National Park Service (NPS)
- Bureau of Safety and Environmental Enforcement (BSEE)
 We selected sites to ensure that our technical testing covered the OCIO and
 Verizon security monitoring and enforcement tools installed at each of the four

primary departmental TICs located in Denver, CO; Reston, VA; Sioux Falls, ID; and Menlo Park, CA. The sites we visited included the following:

- U.S. Bureau of Reclamation (USBR) Headquarters, Denver Federal Center
- U.S. Geological Survey (USGS) Patuxent Wildlife Research Center
- USGS Earth Resources Observation and Science (EROS) Center
- BSEE Headquarters
- FWS National Conservation Training Center (NCTC)
- FWS San Luis National Wildlife Refuge
- NPS Yosemite National Park
- BLM Central California District Office
- Bureau of Indian Affairs (BIA) CONOPS Networks at FWS NCTC

Additional details on our technical testing can be found in Appendix 2.

We conducted our evaluation in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

Appendix 2: Technical Testing Details

We performed technical testing at nine bureau locations within the Department's network to determine the Office of the Chief Information Officer's (OCIO's) ability to detect, prevent, and respond to various types of incidents.

The Department's Cyber Security Operations Section Chief and bureau Associate Chief Information Security Officers (ACISOs) were aware of the testing, but individual incident responders were not informed of the type testing we were performing, or when and where we would conduct the tests. We performed three types of tests, and analyzed the results using both our own tools and our limited access to the OCIO's tools. We were not granted access to all of the OCIO's enterprise incident response tools.

Our tests were designed to simulate exfiltration of sensitive data, compromised machines on the network, and an active malicious threat inside of the network. We analyzed data from the OCIO's tools to determine if it was able to detect or prevent our activity. We requested data from the OCIO's incident responders to determine if there was a human response to our activity. We also used our own tools to monitor our testing activity.

Data Exfiltration Simulation

We created sample Microsoft Word and Microsoft Excel Documents that contained simulated Personally Identifiable Information (PII). These documents each had 10, 100, 1,500 and 10,000 fake credit card numbers and social security numbers. Each document also had a cover page that contained our project number and a request to contact us if recovered. We simulated data exfiltration by transferring these documents to a cloud-based system managed by our team using several methods.

Malware Simulation

During our initial site visits, we configured vulnerability scanning software to use known malware user agents and performed a scan against our cloud-based system. We did this to determine what was necessary to gain the attention of incident responders. We stopped performing this test after we were identified by incident responders.

We used a copy of an easily detectable, generic ransomware executable for the malware download simulation. We disguised the malware by embedding it within several zip files containing other non-malicious files of varying sizes and folder depths, and changing the name of each file after each visit. To simulate malware being delivered to a Department machine, we transferred the ransomware executable and various zip files between our test machines and our cloud-based test system. Because we did not use an infected system, we utilized online tools to

determine the behavior the ransomware would exhibit, if executed, and then performed manual tests to simulate execution.

We also used an open source SSL and SSL IP blacklist to obtain a list of current malicious websites acting as command and control servers for compromised systems. We performed manual tests to simulate an end user connecting to and successfully establishing an encrypted session.

Malicious Actor Simulation

We performed tests to simulate a malicious actor on the network. This scenario includes both a local intruder that gains physical access to the network or a remote intruder that gains access through hacking. We simulated network reconnaissance and pivoting activities against targets on the local network, the bureau's network, and other bureau networks. We used vulnerability scanning software to scan specific Intranet servers located in bureau DMZ networks.

Appendix 3: Response to Draft Report

The Department's response to our draft report follows on page 39.



United States Department of the Interior

OFFICE OF THE SECRETARY Washington, DC 20240

FFB 1 4 2018

Memorandum

To:

Mary L. Kendall

Deputy Inspector General

From:

Sylvia Burns

Chief Information Officer

Subject:

Management Response to the Draft Evaluation Report - Interior Incident Response

Sylvin Bruns

Program Calls for Improvement, 2016-ITA-020 (Report)

Thank you for the opportunity to review and comment on the January 2, 2017, draft report. The Office of the Chief Information Officer (OCIO) concurs with the report recommendations. OCIO is pleased to provide a coordinated Department and bureau-office response with Corrective Action Plans (CAP) and Target Completion dates as Attachment 1.

Please contact me at (202) 208-6194, if you have questions. Your staff may contact Richard Westmark, Chief, Compliance and Audit Management (CAM) Branch at (202) 513-0749.

Attachment:

1. The Department of the Interior's Management Response to the Draft Evaluation Report - Interior Incident Response Program Calls for Improvement, 2016-ITA-020 (Report)

cc: Douglas A. Glenn, Deputy Chief Financial Officer and Director Office of Financial Management

KPMG LLP, 1676 International Drive, McLean, VA 22102 Richard Westmark, Chief, Compliance and Audit Management Morgan Aronson, Director, Financial Audits, Office of Inspector General

Office of the Chief Information Officer

Statement of Actions to Address Office of Inspector General Draft Evaluation Report Interior Incident Response Program Calls for Improvement, Report No. 2016-ITA-020

We recommend that the Department:

Recommendation 1: Create a comprehensive policy, as described by NIST guidance, for the incident response security program that prescribes:

- Organizational priorities
- Roles, responsibilities, and levels of authority
- Performance measures
- Reporting requirements

Response: Concur. OCIO, along with bureau-office information assurance leadership, will take a unified approach to creating a standard comprehensive policy to be followed DOI-wide. The updated policy will include guidance on how priorities, roles, responsibilities, authorities, measures and reporting will be defined, implemented, and managed across all bureaus and offices within the DOI. Similar bureau-specific policies will be retired.

Responsible Official & Title: Stacy Richkun, Branch Chief, Information Assurance Policy, Security Architecture, Security Training and Risk Management (IAPATRM)

Lead Contact & Title: Robert Porter, Information Security Policy, IAPATRM

Target Completion Date: 12/1/2018

Recommendation 2: Utilize the Department's High-Value IT Asset list to develop prioritized event monitoring and incident response activities.

Response: Concur. The DOI OCIO, together with bureau and office IMT leadership, are currently working, as part of the Continuous Diagnostics and Mitigation (CDM) Phase 3 initiative, to implement a single enterprise Security Incident and Event Manager (SIEM) solution. The Department will develop prioritized monitoring and incident response activities for all DOI and bureau and office High Value Assets (HVAs) and other mission-critical systems as part of this initiative. See response to Recommendation 8.

Responsible Official & Title: Stacy Richkun, Branch Chief, IAPATRM

Lead Contact & Title: Maria Clark, Enterprise Risk Management

Target Completion Date: 06/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle)

Recommendation 3: Develop a Department-level incident response plan and procedures that incorporate:

- Strategies and goals, to include metrics for measuring effectiveness
- Incident response team structure
- Communication plans

Response: Concur. The Department of the Interior-Computer Incident Response Center (DOI-CIRC) team developed a Department-level Incident Response (IR) Plan following NIST's guidelines in 2017. The plan was signed on August 28, 2017, by the Department CIO. The IR Plan will be updated to incorporate the centralized requirements described in the policy in Recommendation 1: Strategies and goals, including metrics for measuring effectiveness; incident response team structure; and communication plans.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Response Manager

Target Completion Date: 06/01/2019

Recommendation 4: Review bureau-specific incident response plans and procedures to ensure alignment with the Department's incident response plan.

Response: Concur. Bureaus will abide by the updated the DOI incident response plan. Bureau-specific incident response requirements will be incorporated into the DOI's incident response plan. Once complete, all bureau-specific incident response plans and procedures will be retired.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Response Manager

Target Completion Date: 06/01/2019

Recommendation 5: Develop a solution for providing bureaus consistent access to the enterprise incident response tools, and provide additional event analysis in the interim.

Response: Concur. A solution is currently being developed to provide bureaus and offices secure remote access to unified incident response tools and event analysis.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Robert Lewis, Enterprise Threat Manager

Target Completion Date: 12/1/2018

Recommendation 6: Identify areas of high risk on the Enterprise Services Network (ESN), (e.g. data centers, science centers, DMZ networks) and extend enterprise incident response tool visibility to those areas.

Response: Concur. The DOI will identify areas of high risk on the ESN. The DOI will extend enterprise tools to higher risk enclaves, such as data centers and key ESN points, to improve coverage as indicated in the report. See response to Recommendation 8.

Responsible Official & Title: Stacy Richkun

Lead Contact & Title: Robert Lewis, Enterprise Threat Manager

Target Completion Date: 6/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle.)

Recommendation 7: Require all security incidents be tracked in a single enterprise system that allows Department-wide incident correlation.

Response: Concur. The recently released DOI enterprise IR plan contains a mandate to use the current centralized security incident portal for all incidents defined by NIST. The DOI will reinforce this by issuing guidance to bureau CSIRT personnel.

Responsible Official & Title: Ouentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/1/2018

Recommendation 8: Accelerate plans to implement a Security Incident and Event Manager (SIEM) that can analyze and correlate events across multiple, disparate systems that incorporates data feeds from all security tools and infrastructure systems, to include those managed by the bureaus or third-party contractors.

Response: Concur. Current and previous fiscal constraints precluded the DOI from acquiring an enterprise SIEM within fiscal years 2016-2021. The DOI will obtain a centrally managed enterprise SIEM through CDM Phase 3, for which DHS will provide initial funding. CDM Phase 3 addresses boundary protection and event management for managing the security lifecycle. Specifically, Phase 3 will provide DOI with the ability to strengthen the management of cybersecurity events/incidents and enhance protection of our internet-facing network perimeter borders and security lifecycle. OCIO will

seek funding through the Working Capital Fund to support ongoing operations and maintenance costs after the implementation of CDM Phase 3.

Responsible Official & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Lead Contact & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Target Completion Date: 6/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle)

Recommendation 9: Evaluate security tools with overlapping capabilities, such as antivirus and firewalls, for consolidation to reduce the number of disparate log management and alerting systems.

Response: Concur. The DOI will develop an architectural roadmap for overlapping and unique capabilities at the Department, bureau and office levels, indicating the tools used at each level, and a migration path to unify consistent tool usage without overlap, where possible. Centralizing and reducing the number of log management and alerting systems will result in cost savings, including labor reduction.

Responsible Official & Title: Al Foster, Chief, Information Assurance Operations Branch

Lead Contact & Title: Quentin Cheuk, Cybersecurity Operations Manager

Target Completion Date: 12/31/2021 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities by 6/20/2023 as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle. This earlier date is based on pre-work needed to inform the CDM Phase 3 deployment scope.)

Recommendation 10: Define and enforce minimum Departmentwide standards on log collection and retention that are sufficient for performing event and security incident analysis.

Response: Concur. A Department-wide standard for log collection and retention has been created and is currently under review. It will support the planned centralized SIEM. See response to Recommendation 8.

Responsible Official & Title: Stacy Richkun, Branch Chief, IAPATRM

Lead Contact & Title: Robert Porter, Information Security Policy, IAPATRM

Target Completion Date: 6/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle)

Recommendation 11: Develop a dedicated group of incident responders to perform threat hunting and containment activities with:

- Advanced analytical experience across multiple disciplines
- Authority to access Department-wide event data
- Authority to engage organizationally segregated IT staff

Response: Concur. The DOI will leverage existing resources to develop an enterprise threat hunting capability focused on advanced analytical experience across multiple disciplines with authority to access Department-wide event data, and authority to engage organizationally segregated IT staff.

Responsible Official & Title: Al Foster, Chief, Information Assurance Operations Branch

Lead Contact & Title: Quenten Cheuk, Cybersecurity Operations Manager

Target Completion Date: 12/31/2018

Recommendation 12: Develop Department wide methodology to address inappropriate and prohibited internet usage, to include departmental monitoring and a risk analysis of events.

Response: Concur. The DOI will address this recommendation through a combination of additional user training, and policy review of current internet usage policy with focus on what protocols and sites are allowed for user access, as well as more reliance on automated monitoring of user activity. Automated centralized monitoring of user activity will be provided by future deployment of an SSL/TLS visibility capability and FortiGate follow-on phases that will include Digital Loss Protection (DLP) functionality.

Responsible Official & Title: Stacy Richkun, Branch Chief, Information Assurance Policy, Security Architecture, Security Training and Risk Management (IAPATRM)

Lead Contact & Title: Robert Porter, Information Security Policy, IAPATRM

Target Completion Date: 6/30/2019

Recommendation 13: Configure DLP systems to block the transfer of sensitive information.

Response: Concur. Enabling unified DLP capabilities of the FortiGate appliances at the DOI's Trusted Internet Connection (TIC) is on a future phase of the current implementation.

Responsible Official & Title: Stuart Ott, Chief, Enterprise Infrastructure Services

Lead Contact & Title: Dana Hanson, EIS Project Manager

Target Completion Date: 6/30/2019

Recommendation 14: Ensure all DLP systems provide sufficient data to consolidate information for incident responders to accurately identify and assess the impact of potential incidents.

Response: Concur. Enabling DLP capabilities of the FortiGate appliances at the DOI's TICs will provide consolidated information in a future phase of our current implementation.

Responsible Official & Title: Stuart Ott, Chief, Enterprise Infrastructure Services

Lead Contact & Title: Dana Hanson, EIS Project Manager

Target Completion Date: 6/30/2019

Recommendation 15: Ensure DMZs are configured to log and report events to a centralized SIEM.

Response: Concur. Logs from Demilitarization Zones (DMZ's) will be sent to a centrally managed SIEM solution as described in the response to Recommendation 8.

Responsible Official & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio Management Branch

Lead Contact & Title: Ben Liberty, CDM Program Manager

Target Completion Date: 6/30/2023 (This date is estimated based on DHS deployment of anticipated enterprise SIEM capabilities as part of CDM Phase 3: Boundary Protection and Event Management for Managing the Security Lifecycle)

Recommendation 16: Define a Department-wide baseline of inbound and outbound TIC firewall rules that incorporates:

- Least privilege principle
- Inbound rules to terminate at a DMZ, not internal networks
- Periodic testing to validate that rules are operating as intended

Response: Concur. The DOI will define a singular baseline/standard for TIC firewall rules based on current NIST best practice, ports, protocols, and services documentation. The DOI will engineer a solution that terminates inbound rules at the DOI DMZ. The DOI will remove outdated firewall rules. The DOI will test and validate firewall rules periodically.

Responsible Official & Title: Stuart Ott, Chief, Enterprise Infrastructure Services

Lead Contact & Title: Dana Hanson, EIS Project Manager

Target Completion Date: 6/30/2021 (DOI will incorporate this requirement into the Enterprise Infrastructure Services (EIS) contract recompete, including implementing a new firewall change management system.)

Recommendation 17: Validate that all TIC firewall rules have a currently valid business case and a risk analysis, and remove those that do not.

Response: Concur. The DOI will initiate a project to validate and cleanup all TIC firewall rules.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Michael Klosterman, Enterprise Software, SIEM, Analytics, and Testing (SWAT) Manager

Target Completion Date: 6/30/2021 (DOI will incorporate this requirement into the Enterprise Infrastructure Services (EIS) contract recompete, including implementing a new firewall change management system.)

Recommendation 18: Identify external connections that are not visible to enterprise incident response tools and migrate them to the TIC.

Response: Concur. The DOI will identify connections not traversing the TICs and migrate them to one of the DOI TIC gateways.

Responsible Official & Title: Stuart Ott, Chief, Enterprise Infrastructure Services

Lead Contact & Title: Dana Hanson, EIS Project Manager

Target Completion Date: 6/30/2021 (DOI will incorporate this requirement into the Enterprise Infrastructure Services (EIS) contract recompete, including implementing a new firewall change management system.)

Recommendation 19: Replace or redesign the official incident tracking system, as described by NIST guidance, to include:

- All required metrics
- All phases of the incident response lifecycle
- Security controls applicable to all stored data types

Response: Concur. The DOI will survey existing bureau and office ticketing systems to find a suitable enterprise replacement tracking system that meets NIST requirements, above. Additionally, the DOI will closely monitor the CDM program for the availability of an advanced incident tracking system.

Responsible Official & Title: Kris Caylor, Chief, Strategic and Capital Planning & Portfolio

Management Branch

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/31/2019

Recommendation 20: Provide periodic training to incident response teams on the appropriate and consistent use of the incident tracking system.

Response: Concur. The DOI will provide standard periodic training to all bureau and office incident response teams on the appropriate and consistent use of the incident tracking system. A link with further guidance will be placed into the Department IR Plan to further aide bureaus in the consistent use of the incident portal.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/30/2018

Recommendation 21: Require change control events be processed and recorded in official change control management systems instead of in the official incident tracking system.

Response: Concur. The DOI will no longer input change control events into the DOI-CIRC portal and will leverage the centralized ESN Change Management portal instead.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 02/28/2018

Recommendation 22: Develop processes for periodically performing lessons-learned activities and implement program improvements where warranted.

Response: Concur. The DOI will develop processes for periodically performing DOI-wide lessons learned activities with bureau/office participation and implement program improvements. These processes will include augmenting the Enterprise IR plan with additional lessons learned guidance and adding a capability within the IR portal to record details of lessons learned activity.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/31/2018

Recommendation 23: Develop and implement a quality control program that periodically reviews tracked incidents to ensure they include documentation and analysis of the extent, impact, and mitigation activities.

Response: Concur. The DOI will implement an enterprise quality control program that will include periodic reviews of incident tickets to ensure that they are remediated properly, in a timely manner, and that mitigation activities are adequately documented when incident tickets are closed.

Responsible Official & Title: Quentin Cheuk, Cybersecurity Operations Manager

Lead Contact & Title: Scott Frye, Enterprise Incident Management Manager

Target Completion Date: 12/31/2018

Appendix 4: Status of Recommendations

In response to our draft report, the Department concurred with all 23 recommendations and stated that it was working to implement them. The response included target dates and an official for each recommendation (see Appendix 3). Based on this response, we consider all 23 recommendations resolved but not implemented. We will forward them to the Office of Policy, Management and Budget to track their implementation.

We understand that some of these recommendations may require significant investment in cyber security infrastructure as well as the recruitment of additional staff, but the intended timeframe to implement these recommendations remains a concern. Five recommendations will not be addressed for more than 5 years, and four recommendations will not be addressed for more than 3 years. In the interim, the Department should consider additional temporary or partial solutions.

Recommendations	Status	Action Required
I - 23	Resolved but not implemented	We will refer these recommendations to the Assistant Secretary for Policy, Management and Budget to track their implementation.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doioig.gov

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



FY 2010 FISMA EVALUATION REPORT

Report No.: ISD-EV-MOA-0001-2010

Table of Contents

Results in Brief	1
Introduction	3
Objective	3
Background	3
Findings	5
IT Inventory	5
Certification and Accreditation	10
Security Configuration Management	16
Incident Response and Reporting	20
Security Training	23
Plan of Action and Milestones	29
Remote Access	32
Account and Identity Management	35
Continuous Monitoring	39
Contingency Planning	43
Oversight of Contractor Systems	45
Conclusion and Recommendations	48
Conclusion	48
Recommendation Summary	48
Appendix 1: Scope and Methodology	51
Scope	51
Methodology	52
Appendix 2: Summary of FISMA Results (FY 2003 to 2010)	53
Appendix 3: Related OIG Reports Management Advisories and Evalua	ations 56

Results in Brief

Our fiscal year (FY) 2010 FISMA Evaluation Report reveals major inconsistencies in the U.S. Department of the Interior's (DOI) Information Technology (IT) security program. These inconsistencies are a reflection of DOI's decentralized approach to governing IT security. Each bureau manages its own security program, as the Department Chief Information Officer does not have the authority to unify and align the Department's IT security program.

We found several DOI systems missing or not clearly identified in inventory databases, and that potentially helpful investments were sitting idle on shelves. We also identified key program areas that are not consistently implemented, such as incident response, configuration management, and remote access.

- Our unannounced tests of DOI's incident response capabilities revealed that social engineering gained us network access and access to sensitive information following requests to reset the passwords of key personnel. We found that these potential security breaches occur without being identified and fragmented reporting processes enable these events to continue
- Our testing revealed that bureaus have installed multiple Web browsers that are not compliant with the Federal Desktop Core Configuration standards.
- We determined that DOI bureaus continue to use multiple remote access solutions to which the Department has no insight. We identified one of these remote solutions, which the Department did not know that the bureau had implemented. The bureau was forced to shut it down until it could be formally documented and risks assessed.

We found that the information that authorizing officials use as the basis for their operating decisions is incomplete and inaccurate. This information, which comes to them in a package containing the system security plan, security assessment reports, and plans of action and milestones, should be complete enough for an authorizing official to assess the risks of operating a system. More than half the packages we found were incomplete or lacked the necessary quality to provide authorizing officials with an accurate view of the system security posture. This inadequacy presents further challenges for the Department as it prepares to meet new National Institute of Standards and Technology requirements to move this process toward ongoing security authorizations.

We also found promising programs in DOI's IT security. One such program requires that all DOI employees and contractors use a personal identity verification card to log into the network. This will significantly increase network and remote access security. To date, 76 percent of employees and 23 percent of contractors are enrolled

Also, the Department launched the DOI Innovation and Efficiency Team (DIET) Initiatives in June 2010. Although DIET is still in the planning stages, this initiative promises to provide long-term solutions to cost efficiency.

Introduction

Increased cyber threats have resulted in the establishment of security standards meant to unify the Federal Information Security Management Act (FISMA) framework for the Federal Government.

Fiscal year (FY) 2010 has seen the greatest changes to FISMA requirements since its inception in 2002. The U.S. Department of the Interior (DOI or Department) have not managed to keep pace. Weaknesses in fundamental areas of the Department's Information Technology (IT) security program remain unresolved.

Objective

This report summarizes the results of our FY 2010 FISMA Evaluation of the Department's IT security program. We evaluated DOI's compliance with the requirements of the Federal Information Security Management Act and related information security policies, procedures, standards, and guidelines. This report also contains recommendations to enhance DOI's information security program and move toward full FISMA compliance.

Background

Congress enacted Title III of the E-Government Act of 2002, Federal Information Security Management Act, in response to concerns about the security of Federal information and IT systems. FISMA's primary intent was to facilitate progress in correcting agency information security deficiencies and improve oversight of Federal information security programs. FISMA § 3545(a) requires the Office of Inspector General (OIG) to perform an annual evaluation of the Department's information security program and practices.

FISMA also requires the Secretary of Commerce to prescribe compulsory, binding standards and guidelines pertaining to Federal information systems. As a component of the Department of Commerce, the National Institute of Standards and Technology (NIST) is required to develop Federal Information Processing Standards, which define the minimum requirements for information security and system security categorizations. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems. NIST introduced two publications in the last year that have significantly changed Federal agency information security programs. The revised guidance includes:

- NIST Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems;" and
- NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations."

These publications updated IT security controls to address cyber threats, emphasize IT risk management and continuous monitoring, and recognize that authorizing officials need to have access to near real-time monitoring. Compliance with FISMA is no longer dependent upon a stagnant certification and accreditation package, rather the requirements have moved toward ongoing information system authorizations.

The Office of Management and Budget (OMB) must report annually to Congress on all Federal agencies' FISMA compliance. OMB used CyberScope as the automated FISMA data collection instrument for reporting on agency compliance. CyberScope contained 11 areas for OIG input in FY 2010:

- Certification and Accreditation Program;
- Status of Security Configuration Management;
- Status of Incident Response and Reporting Program;
- Status of Security Training Program;
- Status of Plans of Action and Milestones Program;
- Status of Remote Access Program;
- Status of Account and Identity Management Program;
- Status of Continuous Monitoring Program;
- Status of Contingency Planning Program;
- Status of Agency Program to Oversee Contractor Systems; and
- Financial Audit.

Enterprise Initiative

The Department launched the DOI Innovation and Efficiency Team (DIET) Initiatives in June 2010 "to identify and implement immediate and long-term solutions to realize cost savings, cost avoidance, cost efficiencies and/or innovations across the DOI IT environment." DIET, which is still in the planning phase, includes objectives and projects that, once implemented, promise to contribute to the IT Security Program.

The DIET Initiatives include:

- Infrastructure consolidation (of facilities, telecom, servers and storage, applications and data, and IT asset inventory);
- Data center consolidation;
- Unified messaging;
- Risk-based Information Security Services;
- Radio site consolidation; and
- Workstation ratio reduction.

Findings

The findings in this evaluation are organized by the 11 Information Technology (IT) security program areas: IT inventory, certification and accreditation, security configuration management, incident response and reporting, security training, plans of action and milestones, remote access, account and identity management, continuous monitoring, contingency planning, and oversight of contractor systems.

We also include all relevant policies, guidance, requirements, regulations, or definitions and answer whether or not the Department's bureaus follow that existing guidance.

IT Inventory

Policy

The U.S. Department of the Interior (DOI or Department) has established a policy for maintaining IT inventory, but confusion over the policy has impacted its accuracy. Managing the DOI IT infrastructure is dependent upon an accurate inventory and provides a foundation for an effective IT security program and FISMA compliance.

The March 2008 DOI IT Security Policy Handbook (Version 3.1), requires bureaus to "track all IT system components and security status by maintaining a comprehensive inventory in the DOI Enterprise Architecture Repository (DEAR)." The Chief Information Officer (CIO) issued a directive establishing DEAR "as the official data source for DOI enterprise architecture artifacts, [and] all DOI information systems." The directive also states that the bureau CIOs are responsible for annual written assurance that data in DEAR is accurate and complete.

DOI also implemented the Cyber Security Assessment Management (CSAM) solution, which identifies IT system inventory. Its primary purpose, however, is to be the official repository for preserving Certification & Accreditation (C&A) Package documentation, Plans of Action and Milestones (POAM), and Internal Control Reviews for each system in inventory. A September 23, 2008 Departmental memorandum, titled "Mandatory Use of the Cyber Security Assessment Management (CSAM) Solution" and signed by the Acting Department CIO, specifies mandatory use and full implementation of the CSAM solution.

On April 27, 2009, we issued a management advisory, "Deficiencies in System Inventory Management," which states that disparities exist between DEAR inventory and the inventory documented in C&A packages. The Department CIO

¹ Office of the Chief Information Officer Directive No. 2009-002, "Population and Maintenance of the Departmental Enterprise Architecture Repository," February 6, 2009.

responded to the management advisory on July 9, 2009, stating corrective action was taken for the discrepancies. The Department also stated that it had "initiated a more robust data harmonization effort." We determined corrective actions were not focused on the systemic process weakness. We identified similar issues in FY 2010.

Our review identified that inaccurate and incomplete system inventory is unreliable for identifying accreditation boundaries. We also found that bureau CIOs are not certifying inventory as policy requires.

System Inventory

DOI has not established clear procedures to consistently manage its IT inventory, which results in confusion among bureaus as to which system is used for maintaining inventory.

During our fieldwork, three bureaus stated that CSAM is the most accurate source of inventory information, but the Department has documented and confirmed that DEAR is the primary system for maintaining IT inventory. Despite weekly data feeds from CSAM to DEAR, the two systems are not reflective of each other and they maintain different data elements.

National Institute of Standards and Technology (NIST) Special Publication 800-37 defines an accreditation boundary² as "all components of an information system to be accredited by an authorizing official." DEAR is used to maintain the Department's accredited IT system inventory and component parts, but bureaus maintain the inventory of component parts inconsistently. DEAR does not present an accurate view of the accreditation boundary and the components, accounting for 253³ accredited systems (which include placeholders for pending and unmatched), while CSAM reflects 270. The component under each accredited system is not identified in inventory.

The bureaus use a wide, and often confusing, array of terms related to inventory management. The Department also has no organization-wide agreement for the definition of "systems," and bureaus use inconsistent criteria when determining how all identifiers are used to manage IT inventory.

Sample of Systems reveal Inventory Discrepancies

Inventory entries into DEAR and CSAM are neither complete nor managed consistently across the Department. Our sample of systems showed:

- Inconsistent identification of inventory
 - The Talent Management System was not included in DEAR inventory and was only entered in CSAM as a minor application

² NIST Special Publication 800-37, Revision 1, states that the term "accreditation boundary" is synonymous with "information system boundary" and "authorization boundary."

³ Based on the "DEAR Certification & Accreditation Boundaries-All C&A Detail" July 13, 2010 report.

- with the Human Resource Management Suite accreditation boundary following our request for documentation. This is not the National Business Center's (NBC) normal process. The Talent Management System is now the only minor application in NBC's system inventory in CSAM;
- ODI has consistently failed to include development systems, such as the Incident Management Analysis and Reporting System, which has been in development since 2004, in inventory. It was added into DEAR and CSAM only after we included this system in our sample;
- The Radio Program General Support System is not in DEAR or CSAM inventory; and
- o The Project Portfolio System is not in DEAR or CSAM inventory.
- Incomplete inventory
 - The National Park Service General Support System (OneGSS) has significant minor applications, such as the Concession Management System, which is not identified with its accreditation boundary in DEAR inventory;
 - The Native American Student Information System does not have any components associated with the system in DEAR inventory, yet a contractor operates a portion of the system;
 - The National Conservation Training Center Local Area Network does not have any minor applications, yet a contractor operates an associated property management system; and
 - The Science and Support System-Low (S&SS-Low) was one of the systems receiving minor applications from two retired U.S. Geological Service (USGS) systems, yet the minor applications are not identifiable in DEAR or CSAM inventory and associated with S&SS Low.
- Sites with no minor applications
 - The Bureau of Land Management (BLM) General Support System (GSS) state, district, and local offices are in DEAR and CSAM inventory with no minor applications; and
 - o NPS OneGSS parks, offices, and centers are in CSAM inventory with no minor applications.
- Minor applications with no sites
 - Office of Surface Mining (OSM) GSS minor applications are in DEAR and CSAM inventory and the security documentation agrees; and
 - Office of the Special Trustee (OST) NET minor applications are in CSAM inventory, but the security documentation does not agree with inventory.

Inaccurate Inventory used for Management Decisions

Management decisions based on incomplete and inaccurate inventory introduce risks to the IT security program. It is not prudent for an authorizing official to

operate a system and assume the risk without a clear understanding and accurate documentation of all components included in the accreditation boundary. Furthermore, each year the bureau CIOs are required to certify that their bureau's DEAR database — an inventory system that is not consistently managed and documented — is accurate and complete. In FY 2010, five bureau CIOs completed DEAR certifications, including U.S. Fish and Wildlife Service (FWS), Minerals Management Service (MMS), NBC, NPS, and Office of Historical Trust Accounting (OHTA). We reviewed the completeness of DEAR inventory for the five bureaus that completed the CIO certification and determined only the MMS system, is in fact accurate and complete.

Accreditation Boundaries

An accreditation boundary identifies the information resources covered by the authorization decision. NIST Special Publication 800-37, Revision 1, changes the term "accreditation boundary" to "authorization boundary" or "information system boundary." The authorization boundary is "the set of information resources allocated to an information system" and "well defined boundaries establish the scope of protection for organizational information systems."

Authorization boundaries are poorly defined and documented throughout much of the Department. Errors and omissions in the DEAR system inventory amplify boundary discrepancies and vague definitions. DEAR, CSAM, and the authorization package do not provide an accurate view of system authorization boundaries. Authorizing officials make decisions to operate systems based on the boundary described in the authorization package and in DEAR inventory. The risks associated with the system are not identifiable if boundaries are not accurately identified.

Contractor Systems

DOI guidance is unclear as to when IT systems or subsystems should be identified as a contractor system in inventory. NIST Special Publication 800-37, Revision 1, defines a Federal information system as "an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency." Contractor systems are to be identified in IT inventory separate from agency-owned systems, but DOI guidance does not specify further criteria for determining if contractor systems or subsystems should be identified in DEAR.

Bureaus do not consistently identify contractor systems inventory. Our sample of systems revealed that the identification of contractor systems is inconsistent when both agency and contractor share in hosting or operations.

Two systems in our sample were identified as contractor systems in inventory. Those systems include:

- The Land Records Information System, which is hosted in a DOI Government facility. The system security plan does not reference contract operators; and
- The OHTA Clifton Gunderson Indian Trust Information System, which is hosted at a contractor facility and operated by contractors.

Three other systems in our sample are fully or partially hosted or operated by contractors and are not identified as contractor systems, including:

- The DOI Enterprise Services Network, which is hosted in a Government facility and primarily operated by contractors, along with some Federal personnel;
- The Native American Student Information System, which is primarily hosted in a Government building in Albuquerque, NM, and partially at a contractor facility in Blaine, MN, where contractors provide system administration and help desk support; and
- The National Conservation Training Center Local Area Network hosted at a Government building and includes a Property Management System that is managed by a guest services contractor.

Not clearly identifying contractor systems has impacts beyond the IT inventory. Authorizing officials receive incomplete descriptions of the systems via the C&A packages, DOI cannot oversee contractors and assure compliance with FISMA security requirements, and contractor data centers are not accurately identified, which causes them to be left out for consideration in the Department's data center consolidation efforts.

Hardware and Software Inventory

Conditions at DOI present persistent challenges to maintaining a valid asset inventory. IT acquisitions for hardware and software are not centralized at all bureaus and controlling what is deployed on the network is difficult. Network access controls are not implemented throughout most of DOI, which means there is not an effective way to control what hardware connects to the network. In addition, the widespread use of local administrator rights enables users to install unauthorized software.

The "Department's C&A Guide Using CSAM" states that asset inventory includes "all hardware and software, including Servers, Workstations, O/S [operating system], software suites, applications, Web functionality, development applications, virus protection, Web tools such as Cold Fusion, VPNs [Virtual Private Network], encryption tool, firmware, modems, hubs, routers, contractor authorized hardware and software, firewalls, IDS [intrusion detection system], scan tools, etc."

The Department has the technical capabilities to identify IT asset inventory, but bureaus impose limitations on the network, which prevents DOI insight into all

bureaus. As a result, asset inventory is not centrally managed and bureaus do not use consistent methods to identify their asset inventories. Some bureaus use automated mechanisms to generate asset inventory reports while other bureaus have a manual process, and one bureau is unable to report.

Recommendations

- I. Standardize the use of terms within CSAM.
- 2. Establish clear guidance for managing IT assets system inventory, including: the identification and documentation of minor applications, the identification (description, hosted, or operated) and documentation of contractor components, a process for adding systems in development to inventory, a process for adding test systems into inventory, and a process for mapping all components to authorization boundaries.
- 3. Establish clear guidance for managing hardware and software asset inventory.

Certification and Accreditation **Policy**

System accreditation is required by the Office of Management and Budget⁴ and is a required FISMA process. Accrediting an information system means a "senior agency official accepts responsibility for the security of the system and is fully accountable for any adverse impacts to the agency if a breach of security occurs," according to the Department's June 2009 "C&A Guide Using CSAM Solution" (Version 2.0). The C&A process documents the system security requirements, security controls, and authorization to operate the system.

In February 2010, NIST issued revised guidance⁵ that transforms the traditional C&A process into a six-step Risk Management Framework, now known as the "security authorization process." In addition, August 2009 guidance modified the required minimum IT security controls for systems. DOI has yet to update its C&A policy to correlate with NIST's revised guidance.

The C&A policies detailed in the DOI IT Security Policy Handbook are based on the traditional C&A processes, now outdated by NIST's February 2010 and August 2009 guidance. The Department also has multiple procedural documents for implementing the C&A process, including the draft "DOI Certification and

⁴ Circular A-130, Appendix III.

⁵ NIST Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems."

⁶ NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations."

Accreditation Guide" (February 4, 2008) and the "DOI C&A Guide using CSAM Solution"

We found that bureaus were aware of the various policy and guidance documents, yet do not have a definitive understanding of which guidance to follow. Confusion over the policy and procedural guidance has impacted the implementation of DOI's C&A program.

FISMA Sample of Systems

The weaknesses we identified in our sample are indicative of a flawed Departmental authorization process. Such issues adversely affect the authorizing official's capability to manage information security system risks. Our review determined most of the C&A packages would not give an authorizing official a comprehensive and valid understanding of the system security posture and could not be relied on to support their decision to authorize the operation of the system.

We reviewed a representative sample of 21 IT systems to assess the Department's C&A process (See Appendix 1: Scope and Methodology for the complete list of systems). Our review revealed noncompliance with DOI procedures, documentation deficiencies, invalid accreditations, complex systems not identifying and describing component parts, untimely updates of system security plans, and self assessment of controls and contingency plans.

Our review was based on data provided by bureaus and artifacts from CSAM. CSAM is the official repository for C&A packages, POAM, and Internal Control Reviews for each accredited system in inventory.

CSAM experienced a system failure and backup glitch that had a major impact on the completeness and accuracy of the data in CSAM. The Department CIO stated on July 2, 2010, "Unfortunately, analysis has revealed a breakdown in database backup processes and procedures resulting in loss of data entered into CSAM since approximately February 19, 2010." Since our FY 2010 FIMSA Evaluation was underway during that time, some of our findings may have been impacted. Commonalities we identified in the sample of systems included weaknesses in documentation, system accreditation, control reviews, and contingency plan tests.

Documentation

We found that C&A documentation is done inconsistently and lacks quality. We assessed the C&A packages for our systems sample and determined an overall quality rating of "good," "satisfactory," or "poor." The ratings were based on sufficiency and completeness of detail within the package, compliance with NIST and Departmental guidance, and document organization. Our primary focus was to see if the package provided an authorizing official with an accurate understanding of the system security posture to make valid decisions to operate the system. We found security documentation that showed 62 percent of the 21

systems were in the "poor" category, 24 percent were "satisfactory," and only 14 percent were "good."

Some C&A packages were generated using the CSAM system capabilities, while others were produced independently. The packages generated using CSAM generally lacked tailoring and system-specific detail. CSAM is capable of generating a complete authorization package, but the end result is only as good as the original data entered. We found that portions of the system security plans were missing information and only displayed templates or placeholders. We also identified system security plans with broken hyperlinks, generic responses, limited or no documented update history, and blank signature pages for system security plan approval. Packages produced independently of CSAM were found to be more complete and the documents were reviewed for quality.

System Accreditation

During our evaluation of the FISMA sample of systems, we indentified varying issues with system accreditation. We noticed several weaknesses with the documentation and the process. Problems include:

- Not all systems are accredited;
- The accreditation process for systems in development is unclear;
- Component parts are not fully identified within a larger accreditation boundary; and
- Not all accreditations are completed on time. Furthermore, minimum controls have not been implemented following NIST revisions in August 2009.

Accreditation Problems and Weaknesses

First, not all Department systems are accredited. We identified three systems (Radio, Project Portfolio Management, and S&SS-Low) that are deployed in the DOI environment to varying extents and determined that they are neither covered under valid security authorizations, nor fully identifiable in the DEAR IT inventory.

The Radio Systems Program accreditation has not been completed to date. Radio systems are used in various missions by the Bureau of Indian Affairs (BIA), BLM, FWS, NPS, Bureau of Reclamation (USBR), and USGS. Since the DOI Radio System Program was one of the systems in our sample, we requested security documentation on December 17, 2009, and were informed the consolidated program or bureaus' instances do not have supporting C&A packages. The Office of Management and Budget classifies radio systems as a General Support System, and they must adhere to FISMA requirements, including system accreditation. DOI established the Radio Site Consolidation project charter on June 18, 2010, to analyze alternatives and the feasibility of restructuring the program, but accreditation has not been completed.

Project Portfolio Management does not have a valid accreditation. The system is used by the DOI investment review board and is not included in DEAR inventory or CSAM. We did not receive a response from the Office of the Secretary (OS) regarding our request for system documentation.

The Science and Support System-Low (S&SS-Low) accreditation has not been completed. During our FY 2009 FISMA evaluation, we expressed concerns about the accreditations of two USGS systems: the Office Automation General and Office Automation Specialized. The Associate Director for Geospatial Information and CIO stated on June 12, 2009, that "in accordance with the boundary change certificate memo, the subject systems will have all Assets or constituent subsystem-level components realigned into new systems, therefore decommissioning the old systems is required." Our FY 2010 sample included two systems (S&SS-Low and S&SS-Moderate) on the receiving end of this USGS component realignment. We are unable to reconcile the asset realignment and gain assurance that all component systems are properly accredited for this evaluation.

Second, the Department's guidance regarding the accreditation process for systems in development is unclear. The Department's C&A Guide elaborates on the Clinger-Cohen Act, which "directs the heads of agencies to 'incorporate information security principles and practices throughout the lifecycles of the agency's information systems," by stating, "Therefore, any automated information resource under development, and at any stage during operation and maintenance through disposal, must be included in the security requirements of the system."

We included one such system in our sample to gain an understanding of how the authorization process is implemented during system development. We found that the system, Incident Management and Analysis and Reporting System (IMARS), which is being created to provide a Department-wide information collection, analysis, and reporting system for law enforcement and non-law enforcement, lacks proper documentation and does not have a timely accreditation process underway. The system has been in various stages of development since 2004 but the security documentation process has not moved forward. IMARS is on the Office of Management and Budget's FY 2010 high risk information technology projects list. The necessary security considerations have not been documented.

When we requested the C&A package for the IMARS system, we received a memorandum from the authorizing official with a brief status update, which did not detail the NIST defined tasks that should be underway. Also, the

13

⁷ NIST Special Publication 800-37, Revision 1 (page 5), describes the process for managing information systems-related risks, including, "integrating information security requirements into system development life cycle." Many of the tasks associated with the system's authorization process are detailed in NIST 800-37 and begin during system development.

Department's official repository for C&A package documentation, CSAM, does not contain any security-related documentation for the system.

Third, we found that component parts are not fully and consistently identified within a larger accreditation boundary. When we looked at component parts, or minor applications within complex systems, to determine if they are adequately identified in the accreditation package, we found that the level of detail varied by system size and by bureau.

As an example, inconsistencies were identified between bureaus in how they reflect components in CSAM. The Office of the Secretary successfully and effectively identified the component part (the Talent Management System) within the Human Resource Management Suite major application package. We determined that NPS did not adequately describe the two applications we reviewed. The Yosemite Wilderness Permit System and the Concession Management System were neither described in detail nor clearly identified in the related GSS accreditation package.

Also, despite guidance from the CSAM C&A Guide, the Concession Management System minor application is not fully identifiable in DEAR and associated with the NPS OneGSS. Both NPS minor applications are not fully described in the system security plan, security categorization is not documented, and the security controls are not identified for each subsystem component.

Finally, we found reaccreditations that were not completed in a timely manner. NIST states that the maximum authorization period for an information system is 3 years. Four sample systems had accreditations that expired during our evaluation. The reaccreditations were not completed to correspond with the accreditation expiration date. In all instances, the reaccreditations were between 60 and 90 days overdue, as of the date of this report. One date reflected in CSAM showed that the accreditation expired on June 11, 2011, but the signed accreditation memo shows that the accreditation expired on August 7, 2010.

Annual Self Assessments and NIST Revisions

FISMA § 3544(b)(5), requires annual assessments of the effectiveness of information security policies, procedures, practices, and security controls for all systems. The CIO issued a memorandum⁸ with detailed instructions and a methodology for completing annual self-assessments for systems. It included a requirement that CSAM should be used to document all system Internal Control Review assessments for FY 2010. We found that only 67 percent of the bureaus are using CSAM to assess the system IT security controls.

NIST Special Publication 800-53, Revision 3 guidance has not been addressed in DOI guidance. All controls in that guidance have not been implemented. Most C&A packages are based on the second revision (NIST Special Publication 800-

-

⁸ "Internal Control Review Guidance for FY2010," February 24, 2010.

53, Revision 2), instead of the current version, which was released in August 2009. These updates were to be fully implemented by August 2010, but CSAM has not yet been updated. The FY 2010 annual assessments were completed using Revision 2, but the additional controls have not been assessed, and we have no assurance all minimum baseline controls have been implemented.

Also, we identified multiple process weaknesses during our review of self assessments. We did not find a historical record of assessments consistently posted in CSAM, so we were unable to ascertain if all systems had undergone an annual assessment within 12 months of their FY 2009 self assessment. We also found that large and complex systems do not have a methodology to effectively consolidate control assessments when they are completed at multiple sites under the accreditation boundary. Many security controls did not contain any implementation description.

Contingency Plan Testing

We found inadequate contingency plan testing within the Department. Our sample revealed that 67 percent of the system contingency plan tests were either not completed on time or were insufficiently documented. The DOI IT Security Policy Handbook states that bureaus must test the contingency plan for information systems "at least annually using bureau or office developed-tests and exercises to determine the plan's effectiveness and the organization's readiness to execute the plan." We found multiple systems had test date data entered in CSAM, but no artifacts were provided to support the entry. Without comprehensive and well-documented contingency plan tests, DOI is unable to have confidence in their plans.

DOI Compliance Reviews

We found an ineffective compliance review process within the Department. The results from the reviews are often inflated and they are of little benefit to the bureaus.

The Department's Cyber Security Division conducts annual reviews at each bureau as part of the Department's FISMA oversight and compliance efforts. There is overlap between the OIG FISMA Evaluation and Cyber Security Division's compliance reviews; however, the OIG and Cyber Security Division results often disagree.

Our evaluation noted numerous errors and inconsistencies in the bureaus' authorization packages, yet the Cyber Security Division's compliance reviews resulted in perfect, or near perfect, scores. During our fieldwork, bureaus expressed confusion over the differences in our findings and Cyber Security Division's lack thereof. Bureaus further stated that the Cyber Security Division gave them an opportunity to correct identified deficiencies and have their score modified.

Recommendations

- 4. Update DOI's security authorization policy and guidance to incorporate the latest NIST guidance (NIST 800-37, Revision I, and NIST 800-53, Revision 3).
- 5. Merge the multiple DOI security authorization procedural documents into a single document. The guidance should clarify when the authorization process begins in the life cycle, the role of the senior risk executive, and clarify how information system boundaries are to be documented.

Security Configuration Management Policy

Security configuration management is fundamental to the overall success of an information security program. FISMA emphasizes the need for organizations to implement an organization-wide information security program. A March 22, 2007 Office of Management and Budget memorandum directed agencies to comply with Federal Desktop Core Configuration (FDCC) standards, the security configuration standards that were developed by NIST, the Department of Defense, and the Department of Homeland Security, by February 1, 2008. One year after OMB's memorandum, the Department's Office of the Chief Information Officer issued policy in March 2008 requiring all offices to be in full compliance with FDCC standards by September 30, 2008.

Federal Desktop Core Configuration

FDCC standardizes desktop and laptop configurations and is intended to provide a secure, enterprise-wide managed environment. Departmental policies require compliance with FDCC and also that deviations are documented and approved.

We performed technical testing and assessed FDCC compliance by measuring specific standards and configurations settings on the following benchmarks: ⁹

- Windows XP Professional;
- Internet Explorer Version 7; and
- Windows XP Firewall.

We found that the Department was 80 percent compliant ¹⁰ with FDCC benchmarks in 2010, compared to 68 percent compliant in 2009. We also found inconsistencies, however, such as disparate Web browsers, and unapproved

⁹ We assessed compliance with FDCC where bureaus had these three benchmarks available. Not all bureaus employed these benchmarks, so we were unable to test disparate software.

OIG Secure Content Automation Protocol (SCAP) testing did not take into account approved or unapproved deviations.

FDCC deviations. We reviewed the concept of least privilege and its implementation and impact on security configuration management. The inconsistent configurations present a challenge in securing DOI workstations and hinder the Department's ability to monitor FDCC compliance.

We conducted technical testing in June 2010 and found FDCC compliance varies by bureau as demonstrated in Figure 1. We tested all bureaus with the exception of OHA, as technical testing capabilities were not available to test their operating systems. We found differences in FDCC compliance ranging from 58 to 95 percent throughout the bureaus.

Overall Percentage of Compliance with all FDCC Benchmarks

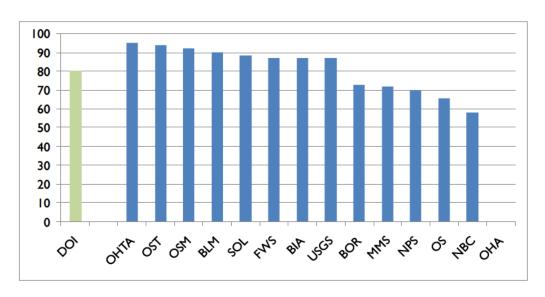


Figure 1. We found differences in FDCC compliance ranging from 58 to 95 percent throughout the bureaus.

Inconsistencies

We identified inconsistencies and unapproved deviations throughout much of the Department during our data analysis. These inconsistencies make monitoring the Department's overall FDCC compliance challenging. We found that:

- BIA, USBR, MMS, and OSM were unable to validate their own compliance with FDCC;
- BLM, FWS, NPS, OHTA, OST, and SOL did not have approved deviations from mandatory FDCC settings;
- MMS, NBC, NPS, Office of the Secretary (OS), and OST do not use the inherent Windows XP firewall, which puts them at risk for not meeting FDCC security requirements;
- USBR, FWS, and USGS do not have firewalls consistently turned on like other bureaus;

- One typical Office of the Secretary user with elevated privileges managed his own FDCC compliance settings instead of receiving the Department's policy through automated mechanisms; and
- One Office of the Secretary user did not have a firewall turned on at any time.

Disparate Web Browsers

We found multiple versions of Web browsers throughout the agency. FDCC mandates that each browser be configured with equivalent FDCC settings, yet we found BIA, BLM, USBR, FWS, MMS, NBC, OS, OSM, and USGS did not configure their additional browsers to be secure. The following table demonstrates the Department's disparate Web browsers:

Disparate Web Browsers by Bureau

Bureau	No. of Browsers Reported	Browsers and Versions Identified
BIA	5	Internet Explorer 7 and Internet Explorer 8; Multiple versions of Mozilla Firefox; Multiple versions of Safari; Netscape Navigator; and Google Chrome
USBR	5	Internet Explorer 6, Internet Explorer 7, and Internet Explorer 8; Multiple versions of Mozilla Firefox; Multiple versions of Safari; Google Chrome versions 1-5; and Opera V9 and V10
BLM	2	Internet Explorer 7 and Mozilla Firefox
FWS	5	Internet Explorer 7 (FWS did not identify the other 4 browsers)
MMS	2	Internet Explorer and multiple versions of Mozilla Firefox
NBC	2	Internet Explorer and Mozilla Firefox
NPS	5	Internet Explorer 7 and Internet Explorer 8; Multiple versions of Mozilla Firefox; Netscape Navigator; Google Chrome; and Opera
OHA	2	Internet Explorer 7 and Internet Explorer 8
OHTA	0	0
OS	2	Internet Explorer and Mozilla Firefox
OSM	2	Internet Explorer and Mozilla Firefox
OST	0	0
SOL	0	0
USGS	5	Internet Explorer, Mozilla Firefox, Safari, Google Chrome, and Opera

Figure 2. These are the browsers that each of the bureaus reported in the OIG data call. In some cases, the number of browsers reported differs from the number actually identified.

Least Privilege and Elevated Rights

FDCC standards prohibit elevated privileges and require least privilege for users, a concept in which users are assigned the absolute minimum privilege necessary to perform required tasks (e.g., "local administrator" or "power user" settings). Assigning elevated privileges, such as "local administrator" or "power user," enable users to circumvent standard configuration controls. According to NIST, any privilege that is not a default user right is an "escalated privilege" and is not in compliance with FDCC.

We found six bureaus that elevated "typical" or "normal" user accounts to "local administrator" or "power users." Moreover, these users are constantly logged in with escalated rights and privileges, thus inviting the opportunity for malicious software (malware) that can damage Department files and settings.

Percentage of Users with Local Administrative Privileges

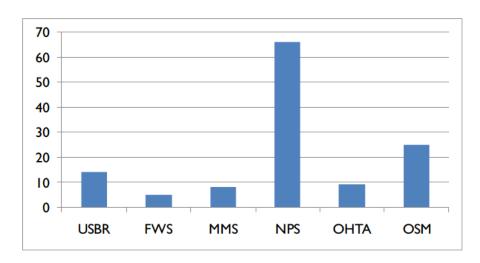


Figure 3. Shows the disparity of percentages of users with elevated privileges, such as "local administrator" or "power user," among bureaus.

Network Access Control

The Department and bureaus have Plan of Action and Milestones¹¹ (POAM) with an estimated cost of \$3 billion to mitigate the weaknesses associated with network access control. Network access control, required per NIST Special Publication 800-53 (IA-3) and Departmental policy, prevents unauthorized devices from connecting to the network by assuring a device is authenticated.

During fieldwork at three bureaus, we determined that network access control was not deployed to prevent unauthorized computers from connecting to the network. We connected an unauthorized computer to the network and performed scanning that was likely to be detected, and little to none of the activity was identified or reported. We were able to connect to internal Web sites containing sensitive information from the unauthorized computer without being authenticated as a DOI or bureau user.

We also found weak physical security controls. ¹² We successfully gained entry and access to offices without any type of identification. Once we were inside bureau facilities, physical access was virtually unrestricted, which enabled logical access to the network. Weak physical security controls coupled with the lack of

¹¹ POAM ID number 13870.

¹² The Incident Response section contains additional information on weak physical security controls.

network access control implementation could lead to the loss or compromise of sensitive information.

Security Technical Implementation Guides

Security technical implementation guides (STIGs) are security configuration checklists or instructions for configuring an application or product to a particular operational environment (e.g., a computer or network devices). Departmental policy requires that STIGs be used as part of the overall security baseline.

The Department's security configuration policy does not address all operating systems and applications in use across the agency. We determined DOI has additional applications for which they do not have applicable STIGs. In addition, we found users with administrator rights who had installed peer-to-peer applications, games, adult content screensavers, and other unauthorized software that went undetected by the Department despite DOI IT Security policy prohibiting it. The Department cannot create a STIG for unidentified software.

Recommendations

- 6. Implement least privilege principal and control use of elevated user rights.
- Standardize Web browsers and firewalls on workstations Interiorwide.
- 8. Document and approve all deviations from FDCC compliance.
- 9. Implement network access controls.

Incident Response and Reporting Policy

FISMA § 3544(a)(7) requires that agencies establish incident response capabilities and have formal procedures to detect, report, and respond to security incidents. Agencies are also required to notify and coordinate their incident response activities with the Department of Homeland Security's U.S. Computer Emergency Readiness Team (US-CERT) and notify and consult with law enforcement agencies, including their respective OIG when necessary based on the guidance. Office of Management and Budget's July 12, 2006 memorandum M-06-09¹³ also requires that agencies report all incidents involving personally identifiable information (PII) to US-CERT within 1 hour of discovering the incident.

¹³ Memorandum M-06-09, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments."

NIST Special Publication 800-61¹⁴ provides guidance for handling IT security incidents. The Interior Computer Security Incident Response Handbook¹⁵ also outlines response and reporting procedures for the agency in sufficient detail, and is consistent with NIST and the DOI IT Security Policy Handbook, which requires bureaus to have an incident response capability.

The Interior Computer Security Incident Response Handbook states that incident response coverage is from 7 a.m. to 7 p.m., Eastern Standard Time. Security Operations personnel act as a point of contact for reporting incidents at the Department and manage the DOI Computer Incident Response Center (CIRC), a centralized database or ticketing system intended to correlate and track incidents at all bureaus.

Procedure Implementation is Lacking

We found that the incident response capability within the Department is fragmented and inconsistent. We identified inconsistencies in how DOI reports incidents to US-CERT. We also identified inconsistencies with bureaus reporting to DOI using the DOI CIRC. We found that bureaus have their own incident-reporting and response policies and procedures, which makes it difficult for the agency to correlate key incidents in a central location. We sampled three bureaus and found that two of them were not aware of the Interior Computer Incident Response Handbook issued in January 2010.

The multiple layers to report an incident to the Department is time intensive and not consistently followed. The lack of a bureau-wide, consolidated approach, coupled with duplicative policy and procedures, is hindering the DOI Incident Response program as a whole.

Absence of Preventative Measures and Breakdown of Procedures

We found that key preventative and incident detection measures were absent and some procedures were disregarded.

Our testing at three bureaus found file and object access not enabled. Having file and object access enabled would allow the bureaus to record and identify OIG or unauthorized personnel's access or attempted access to sensitive information. We found that permissions set to protect sensitive information were generally restrictive throughout the three bureaus but not in all cases. We found that as a domain administrator or local administrator of a server, we were able to view, modify, and copy sensitive information without being detected. We also found weak physical security controls. At a National Park Service headquarters building, we were able to piggyback into the secure facility with an armed Park Ranger through a door for employees only. Once inside, physical access to the bureau facilities was virtually unrestricted, allowing us to gain logical access to the network and collect hardcopy personally identifiable

¹⁵ Version 2, issued on January 28, 2010.

. .

¹⁴ Revision 1, "Computer Security Incident Handling Guide," (March 2008).

information (PII) and sensitive information. Weak physical security controls led to the loss and compromise of hardcopy sensitive information that was never reported to DOI CIRC. We were 100 percent successful in gaining access to three bureau networks with an unauthorized computer. In some cases, we were able to find and access sensitive information with the unauthorized computer.

Logging in with credentials obtained by successful social engineering attacks could have been prevented if two-factor authentication, the use of two independent authentication methods for authorizing secure access to a system, were implemented. We were 100 percent successful at all three bureaus in obtaining usernames or passwords to log into computers. Two-factor authentication was not enforced on these accounts, as we logged in without a Personal Identity Verification card.

We reviewed incidents within the DOI-CIRC from April 21 through September 14, 2010 and found that only three of 245 PII tickets were reported to US-CERT within the required 1-hour timeframe. Of the 245 PII incidents we reviewed within DOI-CIRC, we found that bureaus took an average of 54 days to report PII incidents to the Department, which delayed the Department's required report to US-CERT. Our testing even created an incident in Alaska. We found that our incident was reported to a trained IT security manager within the state, but the IT security manager never reported it to the bureau level. These stovepipes do not allow the centralized management and correlation of incidents to take place in a timely enough manner so that Departmental procedures can be followed.

Incidents

Our testing of incident response at three bureaus demonstrates the inconsistency with which they identify and report incidents. When we created incidents during our testing, we found reporting in one bureau was timely and accurate but untimely and inaccurate in another. We found the following unreported incidents:

- Unauthorized access to facilities;
- Copy and removal of PII from servers;
- Unauthorized access to documents;
- Removal of hardcopy PII-sensitive documents;
- Social engineering attacks;
- Unauthorized scans of networks;
- Unauthorized computers connected to networks; and
- Passwords cracked on files with weak encryption standards.

We also obtained numerous documents and property from NPS, such as:

- Social Security numbers in hardcopy documents, workstations, and servers;
- Numerous users' personal listings of username and passwords in various formats (e.g., MS Excel, MS Word and text files) for GovTrip,

QuickTime, Interior Department Electronic Acquisition System (IDEAS), and the Federal Financial System;

- Numerous credit card numbers and personal receipts attached;
- Social Security numbers posted to internal Web sites of external vendors or providers;
- Adjudication of security clearances;
- 385 IBM Lotus Notes IDs coupled with a password list, which allow unauthorized access to users' email accounts;
- Sensitive information from unlocked shredder bins; and
- An unlocked workstation with a username and password on the screen.

Of these documents and findings, we found neither that the incidents were reported nor any indication that the bureaus knew these documents had been compromised. Our review demonstrated that incidents were not identified and preventative, and detection measures are not fully in place at the Department.

Recommendations

- 10. Implement incident response policies and procedures consistently throughout bureaus and offices.
- II. Require bureaus and offices to use the Department's DOI-CIRC database for incident response and reporting versus their own implementation.

Security Training Policy

FISMA has multiple security training requirements designed to inform personnel of information security risks and responsibilities. DOI's annual security training, Federal Information Systems Security Awareness (FISSA), is required by all users. Role-Based Information Technology Security Training is required by those with significant IT responsibilities. All users must annually acknowledge the Rules of Behavior, which detail users' expected behavior with regard to information and information system use.

DOI's FISSA training consolidates Privacy and Records Management and the annual acknowledgement of the Rules of Behavior. According to the DOI IT Security Policy Handbook, FISSA "is required by all information system users before authorizing access to information systems and annually thereafter." Training requirements reiterated in a December 22, 2009 memorandum from the DOI CIO "require all users of Department of the Interior (DOI) information systems to receive annual information security awareness, privacy, and records management training, as well as acknowledging system Rules of Behavior" by July 31, 2010. An April 21, 2010 Office of Management and Budget

Memorandum (M-10-15) details the FY 2010 FISMA reporting requirements and extends the FISSA training requirement to "each employee," not just system users.

The annual requirement for users to complete the Rules of Behavior agreement was established in the CIO's December 22, 2009 memorandum. The DOI IT Security Policy Handbook also states that bureaus shall "ensure receipt of signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the information system and its resident information." It further states that bureaus "may leverage electronic signatures for use in acknowledging rules of behavior."

FISMA § 3544(a)3(d) requires role-based IT security training. It specifically requires that the Department's CIO train personnel with significant responsibilities for information security. Also, the DOI IT Security Policy Handbook states that role-based information technology security training "programs are implemented in accordance with the DOI Role-Based IT Security Training Guide, and NIST Special Publication 800-16, 'Information Technology Security Training Requirements: A Role- and Performance-Based Model' (March 20, 2009)." On December 23, 2009, the Department CIO released Office of CIO Directive 2010-002, which detailed role-based information technology security training requirements and released DOI's updated Role-Based Security Training Standard Version 2.5 (November 3, 2009). The directive stated that role-based information technology security training requirements were to be completed no later than July 31, 2010.

Results

FISSA

In general, procedures surrounding FISSA training were well implemented during FY 2010. There were challenges associated with the deployment of a new training system, but the guidance remained consistent and well disseminated throughout DOI. July 31, 2010 reports from the Departmental training system reflect that 97.7 percent of Federal employees and other personnel completed the training. The training course covered DOI security policies and procedures and was determined to be comprehensive.

Despite DOI efforts to provide annual training, users continue to introduce risk to the environment. During unannounced fieldwork at a bureau, we observed a contract employee workstation which was left unlocked, unattended, and logged-in to the bureau email. In addition, the email on the screen contained a user name and password to a bureau File Transfer Protocol (FTP) site. Our review of the FISSA completion records revealed that this contractor had been enrolled and included in the baseline but had not completed the FISSA training.

1

¹⁶ Other personnel include all types of non-full time equivalents such as contractors, volunteers, and seasonal employees.

Rules of Behavior

Rules of Behavior for each bureau were included as part of FISSA training. Prior to completing the training, users select the rules of behavior appropriate to their specific bureau. The user is asked to read the rules and select "I agree" to progress and finish the course. During FISMA fieldwork, we confirmed that none of the three bureaus retained signed, hard copy versions of the Rules of Behavior acknowledgement. The DOI IT Security Policy Handbook allows electronic signatures to be associated with the Rules of Behavior acknowledgement. The bureaus that we sampled were unsure if the submission in DOI Learn equates to an electronic signature.

Each bureau has its own Rules of Behavior. We determined that most Rules of Behavior documents do not incorporate specific information regarding remote access or teleworking responsibilities.

Role-Based Security Training

Role-Based Security Training is completed by personnel with significant information security responsibilities. The Department's Role-Based Security Training Standard¹⁷ clearly defines training requirements for each group, bureau responsibilities for tracking completed training, and courses available in DOI Learn. As of July 31, 2010, 54 percent of all personnel required to take role-based security training had completed the required training. The Department extended its reporting date for accepting training completions, and as of September 15, 2010, it reported 96.2 percent completion.

Implementation Challenges

Accurately identifying personnel required to complete FISSA and Role-Based Security training is a challenge for DOI. The Department does not have a central authoritative identity management system for identifying all personnel who have various training requirements. Establishing baselines is a manual process, which provides a point-in-time number based on data from a number of available reports, including the active directory listing, historical training records, payroll, and human resources reports.

Role-based security training completions are tracked in DOI Learn after users "self certify" that they are finished. Supporting artifacts cannot be uploaded into the system as evidence of self certifications. Role-based security training in the Department can only be verified manually, using an extensive data call.

Significant IT Security Duties

Personnel with a range of qualifications and position descriptions perform DOI IT security duties. On December 17, 2009, we issued a data call of all Department personnel with "significant IT security responsibility" to determine the demographics of this group. The list contained employees and non-employees for all bureaus and reflected various portions of their time devoted to IT security

25

¹⁷ Version 2.5, section 1.5, dated November 3, 2009.

duties. The personnel ranged in General Schedule (GS) grade levels and GS-series. The information was manually compiled by each bureau because an automated method does not exist

Our analysis evaluated whether IT security is performed by a sufficient number of personnel with an appropriate grade structure and expertise. The results do not reveal a great deal of consistency regarding personnel and those variables impact how IT security is conducted in DOI.

The Department's Role-Based Security Training Standard¹⁸ defines the type of personnel considered as having "significant information security responsibility." In FY 2010, the Department reported 4,067 personnel with "significant IT security responsibility." Our analysis revealed that:

- 536 more personnel were involved in IT security in FY 2010 than FY 2009;
- 77 percent of the personnel were fulltime Federal employees;
- 23 percent of the personnel were contractors;
- The largest gain in personnel was at USGS, which added 142 employees;
- The next largest gain in personnel was at FWS, which added 128 employees;
- The biggest loss in personnel was at USBR, which lost 13 fulltime employees;
- The number of personnel devoting 100 percent of their time to IT security dropped by 36 percent;
- 50 percent of the new 354 fulltime employees are GS-12 or above;
- IT Security personnel increased by 22 percent from FY 2008; and
- 202 fewer people devote at least 60 percent or more of their time to IT security compared to FY 2009.

Figures 4 to 7 show data from our comparative analysis between FYs 2008, 2009, and 2010.

-

¹⁸ Version 2.5, Section 1.5, dated November 3, 2009.

Personnel Reported (total) Year-by-Year Comparison

	FY	2008	FY	2009		FY :	2010	
Bureau	FTE	CNTR	FTE	CNTR	Total Difference	FTE	CNTR	Total Difference
BIA	127	63	148	46	+4	140	63	+9
BLM	601	123	559	94	-71	572	81	0
BOR	328	16	348	62	+66	335	62	-13
FWS	284	63	273	63	-9	403	63	+128
MMS	192	174	210	109	-47	221	174	+76
NBC	292	141	340	232	+139	389	287	+104
NPS	385	10	408	60	+73	440	57	+29
ОНА	5	5	6	0	-4	6	0	0
OHTA	5	21	5	21	-	4	18	-4
os	56	12	63	18	+13	73	45	+37
OSM	37	10	39	8	-	58	10	+21
OST	17	4	21	0	-	27	0	+6
SOL	2	- 1	6	2	+5	6	3	+1
USGS	327	42	340	48	+19	448	82	+142
Total	2658	685	2768	763		3122	945	
Annual combined total	3	343	3	531	+188	40)67	+536

Figure 4. Presents the number of fulltime Federal employees and contractor personnel in a year-to-year comparison and how they are allocated to various DOI bureaus.

Employees Reported (by Grade) Year-by-Year Comparison

Grade	FY2008	FY2009	FY2010	Difference (FY08-09)	Difference (FY09-10)
SP-5	ı	ı	ı	-	-
WG-11	2	2		-	-1
GS-2			0	-	-1
GS-3	-	2	4	+2	+2
GS-4	4	7	10	+3	+3
GS-5	24	33	37	+9	+4
GS-6	24	18	24	-6	+6
GS-7	95	94	137	-1	+43
GS-8	15	12	15	-3	+3
GS-9	218	228	278	+10	+50
GS-10	5	4	2	-1	-2
GS-11	513	522	589	+9	+67
GS-12	669	665	743	-4	+78
GS/GM- 13	515	562	645	+47	+83
GS/GM- 14	337	366	374	+29	+8
GS/GM- 15	154	171	176	+17	+5
SL	5	4	5	-1	+1
SES	74	76	81	+2	+5
Total	2656	2768	3122	+112	+354

Figure 5. Employees reported by grade, in a year-to-year comparison from FY 2008 to 2010.

Percent of Time Personnel Devoted to IT Security Duties

	FY	2008	FY	2009		FY	2010	
Percentage	FTE	CNTR	FTE	CNTR	Total difference	FTE	CNTR	Total difference
100	506	83	524	153	+88	380	117	-180
≥ 90	531	91	551	160	+89	406	135	-170
≥ 80	549	97	579	165	+98	432	147	-165
≥ 70	626	103	654	182	+107	463	176	-197
≥ 60	652	116	686	190	+108	492	182	-202
≥ 50	783	134	809	214	+106	625	245	-153
≥ 40	845	151	858	221	+83	682	251	-146
≥ 30	1027	193	1008	247	+35	838	285	-132
≥ 20	1467	329	1510	421	+135	1547	572	+188
≥10	2058	517	2208	599	+232	2419	791	+403
≤ 9	600	168	560	164	-44	704	153	+133

Figure 6. The time personnel devote to IT security has dropped dramatically since 2009.

Employees with Significant Information Security Responsibilities

Job Title	Series	Explanation
Clerk (STEP)	0303	IT Clerk (STEP)
Wild Horse and Burro Specialist	0401	System Manager, Wild Horse and Burro System
Natural Resource Specialist	0401	Active Directory Elevated Privileges
Hydrologist	1315	Security Point of Contact
Geologist	1350	IT Security Administration
Supervisory Geologist	1350	IT Security Manager
Fishery Biologist	0482	Security Point of Contact
Geophysicist	1313	IT Security Administration
Physical Scientist	1301	IT Project Manager
Bankcard Coordinator	0303	System Administrator
Realty Specialist	1170	Active Directory Elevated Privileges
Park Ranger	0025	OU Admin, Information Security Management
Electronic Mechanic	2604	Local Area Network Administrator
Supervisory Budget Officer	0340	Budget Tracking
Pipeline Coordinator Officer	0301	System Owner

Figure 7. A considerable array of personnel who perform information security duties have job titles that do not seem to support the necessary qualifications for IT security functions.

Recommendations

- 12. Evaluate the current Rules of Behavior submission process to ensure it satisfies electronic signature requirements.
- 13. Implement a solution that assists in establishing accurate employee and contractor baseline counts, such as a central authoritative identity management system.
- 14. Review the qualifications of personnel performing IT security duties in the Department and reassign those duties accordingly.

Plan of Action and Milestones Policy

The Office of Management and Budget has required quarterly system Plans of Action and Milestones (POAM) since October 31, 2001. The Plan of Action and Milestones program has taken steps forward since then but it certainly has not matured into an effective and reliable program for managing all IT weaknesses in the Department.

The DOI IT Security Policy Handbook requires Bureaus and Offices to develop and continuously update Plan of Action and Milestones for all systems. POAMs should document all planned, implemented, and evaluated remedial actions to correct system deficiencies identified during the assessment of the system security controls. The process is to be completed in accordance with the DOI POAM Process Standard. The Department CIO expanded on the policy on September 23,

2008, when he mandated the use of CSAM as the central database for managing POAMs

Office of Chief Information Officer Directive 2010-006 reiterated this policy on May 18, 2010, and released an updated version on May 10, 2010, "DOI POAM Process Standard" (Version 1.8), incorporating the use of CSAM and automating the process. DOI's June 2009 "C&A Guide using CSAM Solution v2.0" provides additional details and procedures for maintaining the POAM program using the CSAM solution.

According to NIST Special Publication 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," the Plan of Action and Milestones is one of the three key documents in the system authorization package and is used by the authorizing official to monitor progress in correcting weaknesses.

The POAM describes the tasks planned to:

- "Correct any weaknesses or deficiencies in the security controls noted during the assessment;" and
- "Address the residual vulnerabilities in the information system."

It also identifies:

- "The tasks to be accomplished with a recommendation for completion either before or after information system implementation;
- The resources required to accomplish the tasks;
- Any milestones in meeting the tasks; and
- The scheduled completion dates for the milestones."

Policy Implementation

All bureaus have complied with Departmental guidance to use the CSAM solution for system Plans of Action and Milestones. Data in the system could be valuable for management and oversight purposes. We determined that the Department, specifically the Cyber Security Division, has initiated oversight efforts to enhance the data quality within CSAM. The Cyber Security Division sent copies of review items to bureaus, instructing them to take corrective action. Based on our analysis, extensive effort is necessary to enhance the Plan of Action and Milestones data quality. In June 2010, a CSAM system failure was followed by an unsuccessful backup. The Department CIO informed users that data was lost back to approximately February 19, 2010. POAM updates entered in the database during that period of time were impacted, but bureaus were not able to fully assess the impact. During our fieldwork they were still in the process of determining what data was lost.

CSAM automates the Plan of Action and Milestones process and enables the OIG to perform efficient analysis of the data. As with any automated system, the output is only as good as the data input. We identified errors, incomplete information, and missing artifacts associated with the Plan of Action and Milestones. A consolidated October 4, 2010 CSAM Plan of Action and Milestones report for all systems showed:

- The total estimated cost associated with Department Plan of Action and Milestones is more than \$7 billion (\$7,603,531,653);
- Continuous monitoring weaknesses have an estimated \$120.5 million associated cost with limited project investment planning;
- Network access control weaknesses have an estimated \$3 billion associated cost with limited project investment planning;
- 11,064 Plan of Action and Milestones weaknesses are associated with agency systems;
- 1,141 are associated with contractor systems;
- 3,580 are in delayed status;
- 1,330 have not been started:
- 3,227 did not have an estimated associated cost;
- 5,579 of them estimated the cost to be less than \$1,000 each;
- 1,358 Plan of Action and Milestones did not have any milestones;
- 5,808 were completed in an overall average of 277 days (range was 1 to 3,322 days);
- 6,671 did not have an associated artifact posted;
- 16 had blank "detailed weakness descriptions";
- 12 had blank "POAM titles":
- 1,254 had planned finish dates that were blank or to be determined;
- 257 did not include organization priority (i.e., high, medium, or low);
- 487 were identified as mission critical:
- 76 of the 487 mission critical Plan of Action and Milestones were completed on an overall average of 218 days (range was 1 to 868 days);
- 1,634 Plans of Action and Milestones were identified as related to financial systems;
- 853 were missing system status (e.g., development, initiation, operational, or retired); and
- 77 with either incorrect actual start or finish date, as the time to correct was negative.

Using the data above we concluded that bureaus are gathering data in CSAM, but it is not being used to manage IT weaknesses, manage risks, or prioritize corrective action or resource allocation. We further concluded that the data is not being used to perform effective management and oversight of the Plan of Action and Milestones program.

We identified inconsistencies among three bureaus in implementing their Plan of Action and Milestones programs. One of the three bureaus that we reviewed performed further analysis of the data to identify IT controls associated with system Plan of Action and Milestones and various statistics (e.g., delays, milestones, etc.) associated with its Plan of Action and Milestones, but the process was not fully implemented. Bureaus with large, complex systems do not have an established method for combining weaknesses for all component parts of the system. Also, quarterly Plan of Action and Milestones briefings for the authorizing officials are not conducted consistently.

The Impact of CSAM Failure

The Plan of Action and Milestones program was significantly impacted from the CSAM backup failure. During our fieldwork, all three bureaus stated that they experienced data loss and would need additional resources to restore it. Most bureaus were unable to establish a dollar impact but all said it was a big step backward. We were told by one bureau that Plan of Action and Milestones cannot be reentered using historical ID numbers, and therefore tracking capabilities are lost.

Recommendation

15. Ensure that the Department and bureaus are accountable for consistent and accurate data in CSAM to manage Plan of Action and Milestones weaknesses.

Remote Access

Policy

In August 2006, the Chief Information Officer directed all bureaus to transition to the Department's remote access system by January 31, 2007, and a May 2007 Office of Management and Budget memorandum¹⁹ requires two-factor authentication for remote access.

FISMA emphasizes the need for organizations to implement an organization-wide information security program. NIST Special Publication 800-46, Revision 1, "Guide to Enterprise Telework and Remote Access Security," provides details of preparing, operating, and securing remote access solutions.

The DOI IT Security Policy Handbook requires that bureaus mitigate the risk associated with connecting equipment remotely and that access shall be exclusively provided by Government-owned computers. It states the following safeguards must be implemented for remote access:

¹⁹ OMB M-07-16, "Safeguarding against and Responding to the Breach of Personally Identifiable Information."

- Multi-factor authentication;
- Whole disk encryption;
- File and folder encryption;
- Host-based Anti-Virus software;
- Host-based firewall;
- Patch management;
- Security Technical Implementation Guides; and
- Virtual Private Network (VPN) / Encryption of data in transit.

Policy and Telework

The DOI IT Security Policy Handbook provides a set of minimum standard elements for bureaus to address the protection of PII and sensitive data, remote access, and mobile computing device usage in their Rules of Behavior agreement. Copies of bureaus' Rules of Behavior can be accessed in DOI Learn through the training course titled "FY 2010 Annual End-User Federal Information Systems Security Awareness + Privacy and Records Management."

We found a lack of telework or remote access addressed within the Rules of Behavior from bureaus. Also, the Department does not have an up-to-date telework policy addressing security of remote access²⁰ despite a June 2009 revision to NIST Special Publication 800-46, which states that "a telework security policy should define which forms of remote access the organization permits." We did not find this guidance during our review of the Department's telework policy.

Numerous Solutions for Remote Access

Remote Access is noncompliant with the Office of Management and Budget or DOI mandates. More remote access systems have been added against the Department's direction and two-factor authentication has not been fully implemented. These inconsistencies facilitate an unmanageable remote access environment.

Our analysis of remote access systems uncovered a significant vulnerability at FWS. We found that FWS implemented a remote access solution that the Department did not approve to operate. We immediately notified the Department, and it discontinued the remote access system from connecting through the Department until its risks can be formally assessed. Further analysis revealed that FWS called it a "pilot" and had 100 or more users on the remote access system for about 6 months. The Department's Enterprise Infrastructure Division, which monitors and controls the Department's perimeter, was unaware of FWS's remote access solution.

We also found that BLM, NBC, NPS, and USGS maintain and use separate remote access systems, even 3 years after the January 31, 2007 deadline for

 $^{^{20}}$ DOI telework policy has not been updated since Personnel Bulletin No. 05-02 first established one on February 18, 2005.

transitioning to the Department's remote access system. FWS was found to have implemented a new remote access solution this year.

Two-Factor Authentication for Remote Access

DOI cannot enforce two-factor authentication for remote solutions because not all personnel have been issued Personal Identity Verification (PIV) cards²¹ (for more information, see the Account and Identity management section of this report). The Department does not enforce two-factor authentication with users who have that ability.

We reviewed the Department's connections to the DOI centralized remote access solution in August 2010 and found percentages of users using two-factor authentication varied among bureaus. The Department did not have insight into the disparate remote access for those bureaus.

Department-wide, 22 percent of users logged in, in August 2010, using two-factor authentication for remote access. Bureau compliance ranges from 0 to 100 percent in their use of two-factor authentication. The following percentages show bureau compliance with the use of two-factor remote access within the bureaus:

- OHA: 0 percent;
- FWS: less than 1 percent;
- MMS: 2 percent;
- NBC: 2 percent;
- OS: 3 percent;
- NPS: 6 percent;
- BIA: 12 percent;
- BLM: 35 percent;
- USGS: 47 percent;
- OST: 70 percent:
- OHTA: 77 percent;
- USBR: 94 percent; and
- OSM: 100 percent.

Connections to Remote Access

During our interviews at the bureaus, we found that any computer, such as a personal or public library computer can connect to the Department's remote access solution, despite the DOI IT Security Policy Handbook requirement that only Government computers can access the Department's remote access solution. This means that the Department can only enforce one of the eight safeguards: "Virtual Private Network (VPN) / Encryption of data in transit." The Department has no way to validate that personal computers are configured securely. If the Department enables host checking, ²² DOI can reasonably ensure that only

²¹ As of September 30, 2010, 27,326 personnel have yet to be issued PIV cards.

²² Host checking would allow the Department to authorize remote access connections based on criteria such as security configurations.

authorized Government computers with the proper security configurations can connect to DOI remotely.

Recommendations

- 16. Consolidate remote access solutions to allow efficiency and reduce duplicative services.
- 17. Enforce two-factor authentication.
- 18. Enable host checking for remote access.
- 19. Update the telework policy from Personnel Bulletin No. 05-02.

Account and Identity Management Policy

FISMA requires Federal agencies to provide information security for its IT assets. Account and identity management directly correlates with the ability to securely manage IT assets. Homeland Security Presidential Directive 12 mandates the use of standard identification for employees and contractors by October 27, 2009, so as to be compliant with Federal Information Processing Standards²³ and NIST Special Publication 800-63.²⁴

DOI Personnel Bulletin 09-06²⁵ requires compliance with Federal Information Processing Standards 201-1 and Homeland Security Presidential Directive 12. The Chief Information Officer's December 2009 memorandum, "DOI Access Procedures for Bureau/Office Active Directory and Email Systems," recommends that bureaus adhere to new account provisioning procedures and align with DOI Personnel Bulletin 09-06.

The DOI IT Security Policy Handbook requires that bureaus "manage all information system accounts, including establishing, activating, modifying, and reviewing, disabling, and removing accounts..." and "ensure information system accounts are reviewed at least every 3 months."

In a September 27, 2010 management advisory, we expressed concern for simple social engineering techniques that showed a lack of or failure to follow account management procedures. Social engineering results ended in obtaining the username and password for accounts of a Chief Information Security Officer, field office managers, human resources staff, and a domain administrator.

²⁵ "Policy for the Issuance and Management of DOI Access Cards," issued in June 2009.

²³ 201-1, "Personal Identity Verification of Federal Employees and Contractors," issued in March 2006.

²⁴ "Electronic Authentication Guideline," issued in April 2006.

The DOI Access Program

Of the three bureaus we reviewed, we found only one bureau following guidance for account provisioning ²⁶ procedures for the DOI Access system as outlined in the Chief Information Officer's December 2009 memorandum. ²⁷ The procedures, however, are ambiguous because they "recommend" instead of specifically direct the intended procedures. This lack of direction caused confusion, and as a result, the Department is neither compliant with nor fully using the DOI Access system.

Also, we found that account management procedures were duplicative and inconsistently implemented and distributed. A major objective behind the procedures is to create new accounts in the DOI Access System. We found that 9 months after the January 15, 2010 deadline, not all accounts were created within the system.

The DOI Access System cannot provide a full identity management program. It contains contractor status only for contractors with DOI network access but not all DOI contractors require DOI network access. The DOI Access system does not manage access to the copious amount of individual DOI applications. Until all contractors and all disparate DOI applications are considered and entered into DOI Access, the Department will continue to lack one authoritative source for identity management.

Personal Identity Verification (PIV) Cards

Implementing the standard identification mandate from Homeland Security Presidential Directive 12 increases IT security because it ensures that people are who they say they are. Standard identification is a significant element to confirming users' identities because it employs a two-factor authentication, which grants a user access only when they can combine something they have with information that they know (e.g., a Personal Identity Verification card and a password or personal identification number).

The Department reported a December 31, 2010 completion date to the Office of Management and Budget for integration of PIV credentials with logical and physical access systems. We found, however, that the Department has not yet activated PIV cards to 15,682 employees (24 percent) and 11,637 contractors (78 percent) as of September 30, 2010.

The Department considers the following bureaus at risk. A bureau's risk is attributed to PIV card issuance and in some instances, includes employees, contactors, or both:

BIA, which is at 59 percent issuance for employees and 2 percent for contractors;

²⁶ We found OSM at 100 percent compliance, BLM with limited implementation, and NPS testing the procedures at one office. ²⁷ "DOI Access Procedures for Bureau/Office Active Directory and Email Systems."

- BIE, which is at 40 percent issuance for employees and 2 percent for contractors;
- BLM, which is at 73 percent issuance for employees and 2 percent issuance for contractors;
- NPS, which is at 68 percent issuance for employees and 6 percent for contractors;
- FWS, which is at 78 percent issuance for employees and 9 percent for contractors;
- USBR, which is at 60 percent issuance for contractors;
- BOEMRE, which is at 52 percent issuance for contractors;
- OS, which is at 54 percent issuance for contractors; and
- SOL, which is at 24 percent issuance for contractors.

Percent Complete Comp	SPONS (Monthly (EP I: SORSHIP Cumulative) Percent Complete* 106% 106% 101% 115%	ENRO	Percent Complete* 80% 53% 92% 110% 90%	Revised Goal** 2,537 2,075 5,971 4,274 4,936	ent revised g	CTIVATION oal by 12/31/09 ulative) Revised Percent Complete*** 117% 66% 133% 118%	Actual Percent Complete* * 59% 40% 73% 102%
Complete 540 90% 707 90% 874 100% 961 100% 954 97% 668 101% 229 99%	* Actual 5,335 4,362 10,969 5,683 9,316	Percent Complete* 106% 106% 101% 115% 100%	(Monthly 6 Actual 4,039 2,170 9,973 5,471	Percent Complete* 80% 53% 92% 110%	Revised Goal** 2,537 2,075 5,971 4,274	Actual 2,976 1,668 7,938 5,045	Revised Percent Complete*** 117% 66% 133%	Actual Percent Complete* * 59% 40% 73%
Complete 540 90% 707 90% 874 100% 961 100% 954 97% 668 101% 229 99%	5,335 4,362 10,969 5,683 9,316	Percent Complete* 106% 106% 101% 115%	4,039 2,170 9,973 5,471	Percent Complete* 80% 53% 92% 110%	2,537 2,075 5,971 4,274	2,976 1,668 7,938 5,045	Revised Percent Complete*** 117% 66% 133% 118%	Percent Complete* * 59% 40% 73%
Complete 540 90% 707 90% 874 100% 961 100% 954 97% 668 101% 229 99%	5,335 4,362 10,969 5,683 9,316	Complete* 106% 106% 101% 115% 100%	4,039 2,170 9,973 5,471	80% 53% 92% 110%	2,537 2,075 5,971 4,274	2,976 1,668 7,938 5,045	Percent Complete**** 117% 66% 133%	Percent Complete* * 59% 40% 73%
707 90% 874 100% 961 100% 054 97% 668 101% 229 99%	4,362 10,969 5,683 9,316	106% 101% 115% 100%	2,170 9,973 5,471	53% 92% 110%	2,075 5,971 4,274	1,668 7,938 5,045	66% 133% 118%	40% 73%
874 100% 961 100% 054 97% 668 101% 229 99%	10,969 5,683 9,316	101% 115% 100%	9,973 5,471	92% 110%	5,971 4,274	7,938 5,045	133%	73%
961 100% 054 97% 668 101% 229 99%	5,683 9,316	115%	5,471	110%	4,274	5,045	118%	
97% 668 101% 229 99%	9,316	100%						102%
668 101% 229 99 %			8,402	90%	4 924	7.254	1.470/	
229 99%	1,828				7,730	7,234	147%	78%
		111%	1,796	109%	1,447	1,751	121%	106%
	1,220	98%	1,201	96%	1,090	1,140	105%	92%
697 100%	16,455	99%	14,245	85%	13,037	11,305	87%	68%
27 100%	27	100%	27	100%	27	27	100%	100%
78 100%	1,300	133%	1,281	131%	879	1,208	137%	124%
28 100%	585	111%	582	110%	460	548	119%	104%
44 100%	675	105%	667	104%	518	649	125%	101%
15 100%	452	109%	446	107%	414	416	100%	100%
839 100%	9,844	111%	9,088	103%	6,896	7,870	114%	89%
161 98%	68,051	104%	59,388	91%	44,561	49,795	112%	76%
	44 100% 15 100% 339 100% 161 98% * Percent Co. ** Revised Go. *** Percent Co.	44 100% 675 15 100% 452 339 100% 9,844 161 98% 68,051 * Percent Complete = Actual ** Revised Goal = FPPS PP23 e *** Percent Complete = Actual	100% 675 105% 105% 105% 100% 452 109% 100% 9,844 111% 161 98% 68,051 104% Percent Complete = Actual (ASR dated 10-** Revised Goal = FPPS PP23 excluding emplo*** Percent Complete = Actual / Revised Goal 100%	44 100% 675 105% 667 15 100% 452 109% 446 839 100% 9,844 111% 9,088 161 98% 68,051 104% 59,388 ** Percent Complete = Actual (ASR dated 10-04-10) / FPPS 1 *** Revised Goal = FPPS PP23 excluding employees outside complete = Actual / Revised Goal	44 100% 675 105% 667 104% 15 100% 452 109% 446 107% 839 100% 9,844 111% 9,088 103% 161 98% 68,051 104% 59,388 91% ** Percent Complete = Actual (ASR dated 10-04-10) / FPPS PP23 2008 Data *** Revised Goal = FPPS PP23 excluding employees outside of reasonable transport *** Percent Complete = Actual / Revised Goal *** Percent Complete = Actual / Revised Goal	44 100% 675 105% 667 104% 518 15 100% 452 109% 446 107% 414 839 100% 9.844 111% 9.088 103% 6.896 161 98% 68,051 104% 59,388 91% 44,561 ** Percent Complete = Actual (ASR dated 10-04-10) / FPPS PP23 2008 Data *** Revised Goal = FPPS PP23 excluding employees outside of reasonable travel time from *** Percent Complete = Actual / Revised Goal	44 100% 675 105% 667 104% 518 649 15 100% 452 109% 446 107% 414 416 339 100% 9,844 111% 9,088 103% 6,896 7,870 161 98% 68,051 104% 59,388 91% 44,561 49,795 ** Percent Complete = Actual (ASR dated 10-04-10) / FPPS PP23 2008 Data *** Revised Goal = FPPS PP23 excluding employees outside of reasonable travel time from open Creden *** Percent Complete = Actual / Revised Goal	44 100% 675 105% 667 104% 518 649 125% 15 100% 452 109% 446 107% 414 416 100% 339 100% 9,844 111% 9,088 103% 6,896 7,870 114% 161 98% 68,051 104% 59,388 91% 44,561 49,795 112% **Percent Complete = Actual (ASR dated 10-04-10) / FPPS PP23 2008 Data *** **Revised Goal = FPPS PP23 excluding employees outside of reasonable travel time from open Credentialing Centers

0% - 79% At Risk

Figure 8. Percentages exceeding 100 percent are caused by a fluctuating baseline.

DOI ACCESS DASHBOARD FOR CONTRACTORS/AFFILIATES									
Phase II Status as of September 30, 2010									
	NACI Processing			STEP I: SPONSORSHIP (Monthly Cumulative)			ROLLMENT Cumulative)	STEP 3: ACTIVATION (Monthly Cumulative)	
Bureau	OMB QTR REPORT	Actual	Percent Complete*	Actual	Percent Complete*	Actual	Percent Complete*	Actual	Percent Complete*
BIA/BIE	2,850	2,500	88%	196	7%	122	4%	67	2%
BLM	3,750	1,000	27%	134	4%	114	3%	57	2%
BOR	646	640	99%	854	132%	630	98%	385	60%
FWS	745	139	19%	96	13%	82	11%	67	9%
BOEMRE	380	370	97%	295	78%	245	64%	197	52%
NBC	626	527	84%	686	110%	633	101%	513	82%
NPS	3,750	195	5%	316	8%	269	7%	241	6%
ОНТА	408	408	100%	408	100%	382	94%	360	88%
os	354	354	100%	284	80%	273	77%	191	54%
OSM	35	35	100%	43	123%	40	114%	34	97%
OST	150	150	100%	163	109%	155	103%	152	101%
SOL	38	22	58%	29	76%	29	76%	9	24%
USGS	1,187	1,187	100%	1,598	135%	1,334	112%	1,054	89%
Total	14,919	7,527	50%	5,102	34%	4,308	29%	3,327	22%
Percent * Percent Complete = Actual / OMB QTR REPORT complete 90% or more On schedule 80% - 89% Behind									

Percent * Percent Complete = Actual / OMB QTR REPORT	
complete	
90% or more On schedule	
80% - 89% Behind	
0% - 79% At Risk	

Figure 9. Percentages exceeding 100 percent are caused by a fluctuating baseline.

The Department has issued PIV cards to 53,122 employees and contractors, but card use is not enforced. This impacts Departmental privacy, data security, authentication, and overall security posture and causes the Department to fall short of compliance with Homeland Security Presidential Directive 12. Full PIV card compliance would mitigate many of the account management issues addressed in the DOI Access Program section.

Other Fieldwork

Active Directory

We conducted an evaluation of Active Directory in February 2010 to assess the efficiency and effectiveness of its information security controls. Active Directory is a Microsoft technology that provides network services that enable applications to use, find, and manage directory resources such as printers, permissions, and users. It unifies management of IT resources such as security, passwords, users and groups.

We found no standardization for naming conventions, how group policies are structured, creating accounts, or monitoring accounts. In some cases, we even found that a lack of standardization for account management existed within the same bureau.

Capabilities to secure user accounts exist in Active Directory. These capabilities include locking accounts to specific workstations, locking them only to certain hours during the day, or setting them to disable after a certain date. We found that those capabilities were either not consistently implemented or not used at all. We also found training account usernames and passwords on sticky notes posted to workstations, which allows anyone with access to these workstations to log into the account from anywhere in the bureau.

FISMA Fieldwork

We identified inconsistent and poor account management practices during our FISMA review of three bureaus. We found that:

- One NPS helpdesk did not follow procedures for changing passwords;
- Four BLM State helpdesks did not follow procedures for changing passwords, which resulted in four successful social engineering exploits;
- Answers to the BLM National Helpdesk's challenge questions were found on the Internet. These weak questions led to a successful social engineering exploit; and
- The OSM helpdesk did not have adequate procedures to validate users calling in for password changes. We obtained a password for the Chief Information Security Officer.

Recommendations

- 20. Ensure account management procedures adhere to policies.
- 21. Ensure identity verification security questions are unique and answers cannot be easily obtained.
- 22. Issue PIV cards to all employees and contractors.
- 23. Enforce the use of PIV cards for all employees and contractors.

Continuous Monitoring Policy

A continuous monitoring program encompasses all automated and manual processes implemented in the environment to maintain awareness regarding the organization's security posture. According to NIST, "the objective of a continuous monitoring program is to determine if the complete set of planned, required, and deployed security controls within an information system or inherited by the system continue to be effective over time in light of the inevitable changes that occur." Neither DOI nor its bureaus have an established continuous monitoring strategy even though it is required by FISMA.

Continuous monitoring is integral to NIST Special Publication 800-37, ²⁸ Revision 1, and NIST expects the updated guidance to be fully implemented by February 2011. The Office of Management and Budget elaborates in M-10-15, ²⁹ stating that agencies "should develop an enterprise-wide strategy for selecting a subset of their security controls to be monitored on an ongoing basis to ensure all controls are assessed during the 3-year authorization cycle."

Continuous monitoring policies are disparate or lacking at many of the Department's bureaus and offices. We found draft policy at five bureaus, undeveloped policy at three bureaus, and no policy at five bureaus. Without well-defined policies and coordinated procedures for continuous monitoring, the program is fragmented.

Fragmented Continuous Monitoring

The Department and bureaus have Plan of Action and Milestones³⁰ (POAM) with an estimated cost of \$120.5 million to mitigate the weaknesses associated with continuous monitoring.

According to NIST, continuous monitoring programs include: configuration management, security impact analyses on proposed or actual changes, assessments of selected security controls, and active involvement by authorizing officials in the ongoing management of information system security risks. Accomplishing the objectives of the program would require an effective mechanism to update security plans, security assessment reports, and POAM. Also, assessing the ongoing security posture will demand vulnerability scanning tools, network monitoring tools, and other automated support tools that can help determine the security state of an information system.

The Department's Enterprise Infrastructure Division has a multitude of automated capabilities for continuous monitoring, but full implementation has not occurred. Enterprise Services Network, a part of the Enterprise Infrastructure Division, has the technical capabilities to provide continuous monitoring services as detailed in its "Service Catalogue." Bureaus lack consistency as to which services to leverage. We found that DOI fails to integrate data feeds that would facilitate the maturation of the continuous monitoring program. The feeds would encourage a more timely and efficient data collection process.

We found that the Department's Data Loss Prevention system can identify and report personally identifiable information (PII) incidents but cannot prevent them. The system's next phase of implementation is to prevent PII incidents but resource limitations hinder progress. The Enterprise Services Network at the

²⁹ "FY2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management."

²⁸ Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010.

³⁰ Continuous Monitoring POAMs: Department CSAM ID numbers 10918 and 13963; 102 Bureau POAMs associated with 74 systems.

Department's Security Operations Center assesses and manages PII incidents, but it does not have sufficient resources to manage them all. Bureaus assist Departmental personnel by managing their own PII incidents.

We found that only BLM and USGS personnel who manage their bureau's PII incidents are at the Security Operations Center on a fulltime basis. BIA, NPS, OSM, and MMS are managing their incidents at the Security Operations Center on a part-time basis. The remaining bureaus do not assist Security Operations Center personnel with managing PII incidents. More than 200 PII incidents are waiting for remedy within the Department's Data Loss Prevention solution as of September 30, 2010.

Network PII Escalated Incidents by 2,393 NPS 107 67 Bureau **FWS** 31 21 347 BIA 19 18 473 9 9 NBC 105 7 9 (1.5%)OS 125 4 8 USGS 80 6 SOL 30 NPS (53%) USBR 5 3 25 Other 2 3 BOEMRE 15 OSM 109 Info Matches Total

PII Escalated Incidents by Bureau

Figure 10. This is a snapshot of the Department's Data Loss Prevention system from June 1 to September 30, 2010. More than 200 PII incidents are waiting to be remedied.

3,916

202

141

40

21

Our fieldwork at three bureaus also revealed ad hoc continuous monitoring programs. The bureaus would conduct vulnerability scanning, application patching, and vulnerability mitigation as time permitted or urgency demanded. We found that endpoint protection applications were not properly configured to report to a central location so that bureaus could assess the identified situation on time.

We also determined that monitoring software for Active Directory was not configured to monitor significant events associated with user accounts. Risks cannot be assessed and managed if automated systems are not continually monitoring, if data is not analyzed, if trends are not established, and if reports to management personnel are not occurring.

Security Status Reports

To assess risks, authorizing officials need ongoing results from continuous monitoring, updated security plans, security assessment reports, and POAMs. We found only one example of a complete security status report, prepared for Enterprise Services Network, a system in our sample. The reporting, however, did not occur regularly. DOI guidance suggests neither the format nor content for a security status report.

Unused Investments

We found that many continuous monitoring investments are sitting idle or largely unused. A Departmental system called OPNET is capable of mapping the DOI network and identifying IT assets. It can help detect changes in the network infrastructure and provide an accurate and dynamic IT asset inventory for successful continuous monitoring, but these processes have not been completed because bureaus have not agreed to network adjustments that would enable the process.

Not all bureaus have the system configured to report to an application for Active Directory security enhancements, which would assist with monitoring user account management. We also found an asset inventory, auditing, and logging system that can pull hardware and software reports and provide patch management status. This DOI system sits idle because the bureaus have not made the necessary changes to report to the Department.

Recommendations

- 24. Create a comprehensive, enterprise-wide strategy for continuous monitoring.
- 25. Establish a format and content template for the authorizing official's security status reports.
- 26. Enhance the Department's continuous monitoring program using existing investments.
- 27. Ensure that bureaus are reporting to centralized Departmental continuous monitoring systems.
- 28. Establish procedures for using a security assessment report and design a format and content template.

Contingency Planning Policy

FISMA requires that information system contingency plans be part of DOI's IT security program. The DOI IT Security Policy Handbook clearly states that bureaus "develop and implement contingency plans for all information systems." DOI policy also requires annual plan testing and personnel training regarding their roles and responsibilities in executing the plan.

Plans should be documented in accordance with NIST Special Publication 800-34³¹, which addresses contingency planning more extensively than any of the available DOI guidance. According to NIST, guidance must be fully implemented by May 2011.

DOI guidance does not provide DOI system users with adequate information to establish a suite of plans related to the contingency or enough information to understand how their system plan fits into a larger, emergency-preparedness program.³² DOI guidance needs to be improved significantly to assure system contingency plans comply with NIST.

Contingency plans and testing

We found that contingency plans generally are poorly documented, not based on realistic consideration of threats, and have not been annually updated and tested. The plans in our sample described the planning process, rather than realistic threats and proposed measures to reduce their impact.

Information system contingency plan tests are intended to evaluate the viability of a plan, and identify deficiencies and lessons learned. Although FISMA requires annual, documented tests, we found that many testing scenarios were simplistic and provided limited documentation and conclusions to justify the worth of plan testing.

The backup failure associated with the Office of the Chief Information Officer's own CSAM solution was a major setback that exemplifies the importance of contingency plan testing. System backup and recovery procedures are part of contingency planning; they are to be tested annually in accordance with DOI policy. In the case of the CSAM failure, not all bureaus retained duplicate documentation that could be used for restoration. Had CSAM's contingency plan been tested, it is likely the backup "glitch" would have been detected earlier and potentially mitigated its impact.

We found many areas where plans in our sample fell short. Eight plans have not been updated within the last year, as required. One contingency plan had not been

³¹ Revision 1 of NIST Special Publication 800-34, titled "Contingency Planning Guide for Federal Systems," was released in May 2010.

³² "Certification and Accreditation (C&A) Guide Using the Cyber Security Assessment and Management (CSAM) Solution Version 2.0."

updated since 2006. We also identified eight systems that did not conduct timely contingency plan tests and three that failed to provide any artifacts to document the test

We also found that contingency plans for systems with high security categorization also were not tested or updated on time. Specifically, we noted that six of the 10 DOI systems were not tested annually, and seven of the 10 plans were not updated annually as is required for all information system contingency plans.

Large, complex systems have not established a contingency plan or even a strategy to consolidate a plan for General Support Systems. Bureaus with large, complex systems have not documented their process for combining the component plans into a consolidated plan for the entire system. We determined some of the component plans have not been updated since 2004. Outdated contingency plans for the component parts are not useful when considering contingency planning for the whole system.

We found that bureaus' various interpretations of the contingency planning process have resulted in inconsistent implementation. According to NIST Special Publication 800-34, "universally accepted definitions for information system contingency planning and the related planning areas have not been available. Occasionally, this leads to confusion regarding the actual scope and purpose of various types of plans." DOI guidance does not address key contingency planning areas, including business impact analysis, business continuity plans, and disaster recovery plans.

Lack of Integration

During our fieldwork, we asked how the bureaus incorporate their information system contingency plans into their overall risk-management, security, and emergency-preparedness programs. We found that the system contingency plans were not considered as part of the bureaus' or location's emergency-preparedness programs. We found one system contingency plan in our sample had been incorporated into a combined contingency plan for all IT operations at that location. The individual information system contingency plans had been considered in aggregate to establish a larger, integrated plan. DOI is unfamiliar with the concept that a suite of plans would be necessary in the event of a disruption. The response, continuity, recovery, and resumption of mission and business functions and information systems are situational, but bureaus have no comprehensive planning guidance to follow.

Recommendation

29. Update contingency planning guidance to correspond with NIST Special Publication 800-34, Revision 1, before May 2011.

Oversight of Contractor Systems Policy

Overall, Departmental policy regarding contractor oversight is lacking, even though FISMA's requirements for information security also apply to contractor systems, ³³ and responsibility and accountability reside with DOI.

FISMA requirements and contractor oversight are addressed in multiple sources of Federal guidance. Interdependencies exist between the various sources of guidance, and coordinated oversight practices are required to ensure effectiveness. Federal Acquisition Regulations (FAR) emphasize the IT security requirements that are included in acquisition documents. The security requirements are much more extensive than just the clauses included in the acquisition documents. FISMA requires that contractors comply with the contracting agency's IT security policies for their program. NIST and OMB provide guidance for implementing FISMA, which often includes requirements for contractors. All four sources (FAR, agency policies, NIST, and OMB) require oversight of contractors. Focusing on any one of the four sources of guidance narrows contractor oversight requirements and does not address the comprehensiveness of the IT security requirements.

The DOI IT Security Policy Handbook does not address contractor oversight responsibilities beyond the capital planning process. It only includes language to be included with Exhibit 300, the business case submission to the OMB for IT capital projects. Also, Departmental policy neither addresses ongoing oversight responsibilities and how the efforts should be documented nor does it provide clear guidance for identifying contractor systems in inventory (for more information, see the IT Inventory section of this report).

Policy Weaknesses

An April 2005 U.S. Government Accountability Office report identified oversight weaknesses of contractors who provide IT systems and services. ³⁴ Also, independent auditors conducting the FY 2010 DOI Financial System Audit identified contractor monitoring concerns in a Notice of Finding and Recommendation (NFR DOI-2010-0007). Specifically, they found that "DOI does not have a centralized system to accurately track the entire population of contractors with access to Interior's IT systems."

³³ FISMA § 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires that each agency provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source."

³⁴ Report No. GAO-05-362, titled "Information Security: Improving Oversight of Access to Federal Systems and Data by Contractors can Reduce Risk."

Impact

Full identification of contractors and contractor systems is fundamental to contractor oversight responsibilities. DOI Access is issuing PIV cards to 14,947 contractors and, to date, has issued them to only 23 percent of the contractors (see the Identity and Account Management section of this report). The DOI IT system inventory identifies 23 accredited contractor systems. During our review of the sample of systems, however, we found three components with contractor-provided IT services or equipment not clearly identified in DOI IT inventory. Assuring the implementation of oversight procedures is impossible if components are not clearly identified in inventory, just as it is impossible to assure contractor compliance with various FISMA requirements if DOI cannot accurately identify them

Vague guidance statements regarding applicability to contractors are found throughout Department policies. The procedures for contractor oversight are not detailed nor are the documentation requirements defined. We found no clear evidence that the contractor oversight processes have been implemented, but we did see references to contractor operations comingled with agency assessments. Roles and responsibilities for the IT security program elements are not clearly delineated between DOI and contractors.

Bureaus that are required to perform contractor oversight have not established or followed a systematic process, and DOI does not have specific policies for overseeing contractor security practices. The ramifications of not performing contractor oversight significantly impacts identification risk and compliance with FISMA, NIST, Office of Management and Budget, and FAR.

The Department cannot have assurance of its security posture for multiple IT security program areas without contractor oversight of the following:

- Annual assessment of controls at contractor locations;
- Completed IT inventory;
- Security training (role-based security and FISSA training);
- Personnel security (background investigations);
- Physical security (security of data, facility, systems);
- Privileged access to Federal data and systems:
- Oversight of sub-contractors at a contract facility;
- Information controls (privacy) over shared environments;
- Interconnection security agreements and memorandum of understanding;
- The DOI Access process for contractors;
- FDCC compliance;
- Encryption when transporting data;
- Ongoing risk assessments;
- Completions of e-risk authentications; and
- Contractors' system maintenance (e.g., patching, virus protection, scanning, etc.).

Contracting Practices — Hardware and Software Purchases

IT acquisitions are not centrally managed within DOI or bureaus. During fieldwork, we determined that hardware and software purchase generally occur in three ways: under the DOI blanket purchase agreements, General Services Administration schedule (IT Schedule 70), or direct purchase at various bureau levels. We were unable to validate that FAR, parts 39 and 39 D³⁵, were consistently included on contracts managed at the bureau level. During fieldwork, we were told that personnel with direct purchase authority routinely purchase hardware. Such purchases make maintaining an accurate IT Inventory difficult and DOI is not assured they are obtaining secure configurations. We found that copies of contracts for workstation acquisitions did not include FDCC requirements.

We determined that IT security requirements were not consistently included in IT service contracts. We found some security requirements added to some service contracts, but the content varied significantly between bureaus. Furthermore, we determined that the oversight requirements were not specifically referenced or stated

We also found that bureaus purchase software outside of the Department's enterprise license agreements or blanket purchase agreements, so discounted rates are not applied. From 1999 to 2009, bureaus purchased 7 percent of their Adobe products outside of Department contracts. Symantec, an end-point security provider in DOI, stated that "the current enterprise agreement is only about 50 percent" of what the bureaus spend with Symantec annually. Such purchases increase the overall costs associated with software purchases. Without the ability to control software acquisitions, the Department cannot ensure efficient spending and standardized software

Recommendations

- 30. Define, document, and establish procedures for contactor oversight in accordance with FISMA requirements.
- 31. Coordinate between IT security and the associated procurement contracting office.

³⁵ Part 39 of the Federal Acquisition Regulation (FAR) requires agencies to include appropriate information technology security policies and requirements when acquiring information technology, and Part 39d incorporates requirements for using common security configurations.

47

Conclusion and Recommendations

Conclusion

Poor information in management information systems and inconsistent implementation continues to impact the DOI IT security program. Bureaus will remain unaccountable for their IT security shortcomings and inconsistencies will persist until they are required to follow DOI policy and guidance. Fundamental program components must improve or they will continue to struggle to satisfy FISMA requirements.

Recommendation Summary

To address the deficiencies identified in this report, we recommend that DOI:

- 1. Standardize the use of terms within CSAM.
- 2. Establish clear guidance for managing IT assets system inventory, including: the identification and documentation of minor applications, the identification (description, hosted, or operated) and documentation of contractor components, a process for adding systems in development to inventory, a process for adding test systems into inventory, and a process for mapping all components to authorization boundaries.
- 3. Establish clear guidance for managing hardware and software asset inventory.
- 4. Update DOI's security authorization policy and guidance to incorporate the latest NIST guidance (NIST 800-37, Revision 1, and NIST 800-53, Revision 3).
- 5. Merge the multiple DOI security authorization procedural documents into a single document. The guidance should clarify when the authorization process begins in the life cycle, the role of the senior risk executive, and clarify how information system boundaries are to be documented.
- 6. Implement least privilege principal and control use of elevated user rights.
- 7. Standardize Web browsers and firewalls on workstations Interior-wide.
- 8. Document and approve all deviations from FDCC compliance.
- 9. Implement network access controls.
- 10. Implement incident response policies and procedures consistently throughout bureaus and offices.

- 11. Require bureaus and offices to use the Department's DOI CIRC database for incident response and reporting versus their own implementation.
- 12. Evaluate the current Rules of Behavior submission process to ensure it satisfies electronic signature requirements.
- 13. Implement a solution that assists in establishing accurate employee and contractor baseline counts, such as a central authoritative identity management system.
- 14. Review the qualifications of personnel performing IT security duties in the Department and reassign those duties accordingly.
- 15. Ensure that the Department and bureaus are accountable for accurate data in CSAM to manage Plan of Action and Milestones weaknesses.
- 16. Consolidate remote access solutions to allow efficiency and reduce duplicative services.
- 17. Enforce two-factor authentication.
- 18. Enable host checking for remote access.
- 19. Update the telework policy from Personnel Bulletin No. 05-02.
- 20. Ensure account management procedures adhere to policies.
- 21. Ensure identity verification security questions are unique and answers cannot be easily obtained.
- 22. Issue PIV cards to all employees and contractors.
- 23. Enforce the use of PIV cards for all employees and contractors.
- 24. Create a comprehensive, enterprise-wide strategy for continuous monitoring.
- 25. Establish a format and content template for the authorizing official's security status reports.
- 26. Enhance the Department's continuous monitoring program using existing investments.
- 27. Ensure that bureaus are reporting to centralized Departmental continuous monitoring systems.

- 28. Establish procedures for using a security assessment report and design a format and content template.
- 29. Update contingency planning guidance to correspond with NIST Special Publication 800-34, Revision 1, before May 2011.
- 30. Define, document, and establish procedures for contactor oversight in accordance with FISMA requirements.
- 31. Coordinate between IT security and the associated contract procurement office.

Appendix I: Scope and Methodology

Scope

We conducted technical configuration testing at all bureaus, except the Office of Hearings and Appeals, and comprehensive IT security program fieldwork to include interviews, observations, and source documents at three bureaus:

- The National Park Service
 - National Information Technology Center (NITC) and Washington Support Office, Washington, DC, August 30 to September 2, 2010;
 - National Information Service Center, Lakewood, CO, September 15, 2010; and
 - Rocky Mountain National Park, Estes Park, CO, September 20 and 21, 2010.
- The Office of Surface and Mining
 - o Office of the Chief Information Officer, Washington, DC, August 4 to August 6, 2010.
- The Bureau of Land Management
 - Information Resource Management, IT Security Division (WO-590), Washington, DC, July 26 to July 28, 2010.

We selected a sample of 21 systems, which represent accreditation boundaries, components of a larger boundary, or systems identified in the DOI environment.

FISMA Sample of Systems for Fiscal Year 2010

Sample No.	System Name	Acronym	Security Categorization
I	Native American Student Information System	NASIS	moderate
2	Land Records Information System	LRIS	moderate
3	BLM GSS	BLM GSS	moderate
4	LAWNET	LAWNET	moderate
5	NIFCeNET GSS	NIFCeNET	moderate
6	National Conservation Training Center Local Area Network NCTC LAN	NCTC	moderate
7	Talent Management System	TMS	moderate
8	AMAG Physical Acess Control System	AMAG	moderate
9	NPS-GSS (Yosemite Wilderness Permit System)	OneGSS (Permit)	moderate
10	NPS-GSS (Concessions Management System)	OneGSS (Concession)	moderate
11	Technical Information Management System	TIMS	moderate
12	OHTA Clifton Gunderson Indian Trust Information System	OHTA-CGITIS	high
13	DOI Enterprise Services Network	ESN	moderate
14	Incident Management Analysis and Reporting System	IMARS	not categorized
15	Project Portfolio System	PPM	not categorized

16	Radio Systems (BLM, NPS, USGS)	Radio	not categorized
17	OSM Enterprise GSS	OSM-GSS	moderate
18	OST LAN/WAN	OSTNet	moderate
19	SOL-NET	SOL-NET	moderate
20	Science and Support System - Moderate	S&SS-Moderate	moderate
21	Science and Support System - Low	S&SS - Low	low

Within this sample, we looked beyond authorization packages to assess DOI's process for managing all IT system inventory. The authorization packages in our sample included most bureaus, all security categorizations (i.e., high, moderate, and low), and all types of systems (e.g., general support systems, major application, minor applications, and undetermined), operational status (i.e., development and operational), and agency and contractor systems.

We based our analysis on data calls issued to the Department and bureaus during fiscal year 2010. We completed additional analysis using information obtained from two Departmental systems: DOI Enterprise Architecture Repository (DEAR) and Cyber Security Assessment Management (CSAM) solution. We reviewed applicable laws, regulations, Office of Management and Budget guidance, National Institute of Standards and Technology standards, Government Accountability Office reports, and Department and bureau policies. All applicable standards and guidance were used as baselines for assessing the DOI IT security program.

Methodology

FISMA requires agencies to have an annual independent evaluation of their information security program and practices and for agencies to report results of the evaluation to the Office of Management and Budget.

We conducted our FY 2010 FISMA evaluation to obtain information required for Office of Management and Budget reporting. This report consolidates our findings related to the Department of the Interior's IT Security Program and their compliance with key FISMA areas.

We conducted our evaluation in accordance with the "Quality Standards for Inspections" as put forth by the Council of Inspector General on Integrity and Efficiency. Accordingly, we included such tests and other procedures that we considered necessary under the circumstances. The conclusions in this report are based on our fieldwork, technical testing, data calls, and analysis of data in Departmental systems.

Appendix 2: Summary of FISMA Results (FY 2003 to 2010)

DOI spent an estimated \$719.6 million on IT security since fiscal year (FY) 2003, but FISMA noncompliance persists. Continued funding to DOI's IT Security Program as it is structured is inconsistent with OMB's intent according to a December 21, 2004 advisory (A-123, "Management's Responsibility for Internal Control"), which states "management accountability is the expectation that managers are responsible for the quality and timeliness of program performance, increasing productivity, controlling costs and mitigating adverse aspects of agency operations, and assuring that programs are managed with integrity and in compliance with applicable law."

The following is a summary of conclusions from DOI FISMA evaluation reports and the associated IT funding by fiscal year, beginning with 2003.

FY 2003

IT Budget: \$791.2³⁶ million, or 5.7 percent of the DOI's overall budget (\$13,881 million).³⁷

FISMA report conclusion: "We found that the Department continues to make significant progress to improve the security over its information systems. However, its overall security program does not yet adequately protect all information systems supporting the operations and assets of the Department and therefore remains a material weakness."

FY 2004

IT Budget: \$816.5 million, or 5.7 percent of the DOI's overall budget (\$14,325 million).

FISMA report conclusion: "We found that the Department continues to improve the security over its information systems. However, despite sound guidance from the Office of the Chief Information Officer, we continue to identify weaknesses in bureau and office implementation of IT security requirements."

FY 2005

IT Budget: \$802.8 million, or 5.7 percent of the DOI's overall budget (\$15,839 million).

FISMA report conclusion: "We have determined that there are significant weaknesses in DOI's compliance with FISMA, as well as its IT security program as a whole. Our audits, evaluations, and technical testing of DOI's systems and IT security program show that bureaus and offices

³⁷ The total DOI Budget for each fiscal year can be found at http://www.doi.gov/budget.

³⁶ IT Budget was estimated for FY 2003, FY 2004 and FY 2005 using the average of the FY 2006-2009 IT percentages.

are not implementing DOI policies and are not complying with OMB requirements for Certification and Accreditation."

FY 2006

IT Budget: \$934.0 million,³⁸ or roughly 5.8 percent of DOI's overall budget (\$16,122 million).

FISMA report conclusion: "Our testing and evaluation of DOI's IT Security program for Fiscal Year 2006 indicates that DOI has made good progress in the following areas: System Inventory, POA&Ms, Computer Security Incident Response, and Contractor Oversight. Still more work is needed to improve DOI's Certification & Accreditation program and the use of standard security configurations for servers, workstations, databases, and network equipment throughout DOI. Weaknesses in these two critical areas impact a broad set of federal requirements requiring the use of effective management, operational and technical controls."

FY 2007

IT Budget: \$957.6 million, or roughly 6.1 percent of DOI's overall budget (\$15,799 million).

FISMA report conclusion: "DOI made good progress in a number of key FISMA areas; however, our evaluation determined the DOI information security program has not been consistently implemented throughout the Department and the resulting weaknesses hinder achievement of full compliance with FISMA."

FY 2008

IT Budget: \$952.7 million, or roughly 5.4 percent of DOI's overall budget (\$17,475 million).

FISMA report conclusion: "As in the past several years, the Department has made progress in documenting information security; however, implementation lags. There remain fundamental flaws in compliance with the FISMA. Lack of compliance is due in large part to the decentralized nature of the Department, IT program and lack of authority by the Department's CIO. These serious organizational flaws potentially negate the many millions of dollars spent on IT security annually. Lack of departmental oversight, coupled with questionably qualified personnel performing information security duties across the Department, contributes inadequate incident detection and response capabilities put the Department at substantial risk."

FY 2009

IT Budget: \$965 million, or roughly 5.6 percent of DOI's overall budget (\$17,183 million).

FISMA report conclusion: "As in previous years, we found DOI does not fully comply with the FISMA. The decentralized organizational

³⁸ IT Investment Portfolio amounts are from Exhibit 53 for each fiscal year.

structure, fragmented governance processes related to the IT program, lack of oversight, bureau resistance to departmental guidance, and use of substantially under-qualified personnel to perform significant information security duties exasperates the challenges in securing the Department's information and information systems."

FY 2010

IT Budget: \$995.7 million or 8.2 percent of the DOI overall budget (\$12,587 million).

FISMA report conclusion: Poor information in management information systems and inconsistent implementation continues to impact the DOI IT security program. Bureaus will remain unaccountable for their IT security shortcomings and inconsistencies will persist until they are required to follow DOI policy and guidance. Fundamental program components must improve or they will continue to struggle to satisfy FISMA requirements.

FY 2011

IT Budget: \$981.8 million (proposed) or 8.05 percent of the DOI overall budget (\$12,200 million).

Appendix 3: Related OIG Reports, Management Advisories, and Evaluations

A list of summaries and updates, if applicable, for OIG reports and management advisories related to IT's Information Security Program and the fiscal year (FY) 2010 FISMA Evaluation is included below.

FY 2010

Management Advisory: "Account Management," September 27, 2010, documented occurrences of successful social engineering. It identified a lack of user account management procedures resulting in user accounts being compromised and gaining unauthorized network access.

Report: "Evaluation of the Active Directory," No. ISD-EV-MOA-0006-2010, August 2010, documented a lack of standardization in the Active Directory structure, unused investments, and a lack of separation of duties.

Report: "Privacy Impact Assessment," No. ISD-EV-MOA-0005-2010, June 2010, documented inconsistencies in implementing Privacy Impact Assessment requirements. We found processes for Privacy Impact Assessment requirements and Privacy Impact Assessments for IT systems have not been completed to identify privacy risks associated with sensitive information.

Report: "Information Security Evaluation of the National Interagency Fire Center," No. ISD-EV-MOA-0003-2010, June 2010, documented the lack of standardization, duplication, and redundancies at DOI bureaus that are co-located. In addition, radio systems were not certified and accredited.

Management Advisory: "Deficiencies in System Inventory Technology," OIG Case No. PI-PI-10-0045-1, March 2, 2010, documented the lack of accountability for hard drives of former DOI political appointees.

FY 2009

Management Advisory: "Waste and Noncompliance in Departmental Information Systems," October 15, 2009, documented that a vulnerability scanning system is underused and managed inconsistently with FISMA requirements.

Update: No change identified during FY 2010.

Evaluation: "Computer Configuration Evaluation," No. ISD-EV-MOA-0003-2009, August 2009, documented broad noncompliance with

mandatory Federal standards associated with the Federal Desktop Core Configuration as well as OMB and Departmental policy.

Update: We conducted similar testing in FY 2010 and the results are included in this FISMA report.

Management Advisory: "Waste in implementation of Data Encryption Solution," April 8, 2009, documented \$57,000 per month wasted by failing to implement a purchased encryption solution and the additional incurring maintenance costs.

Update: The encryption solution has not yet been fully implemented as of FY 2010.

FY 2008

Report: "Compilation of Information Technology Challenges at the DOI," May 2008, documented the need to rescind Secretarial Order 3244. **Update:** No action has been taken.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in government concern everyone: Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to Departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Mail: U.S. Department of the Interior

Office of Inspector General Mail Stop 4428 MIB 1849 C Street, NW Washington, D.C. 20240

By Phone: 24-Hour Toll Free 800-424-5081

Washington Metro Area 703-487-5435

By Fax: 703-487-5402

By Internet: www.doioig.gov



U.S. DEPARTMENT—OF THE INTERIOR— WEB HOSTING SERVICES



JUN 0 4 2014

Memorandum

To:

Sylvia Burns

Acting Chief Information Officer

From:

Mary L. Kendall

Deputy Inspector General

Subject:

Inspection Report – U.S. Department of the Interior Web Hosting Services

Herdall

Report No. ISD-IS-OCIO-0001-2014

In early January 2014, the U.S. Department of the Interior (DOI) and Office of Inspector General (OIG) websites experienced an extended outage of 7 days. These websites, which are hosted by the National Park Service (NPS), provide critical information to the general public, and their availability contributes to the missions of both DOI and OIG. We initiated an inspection to determine the cause of the outage and to identify whether the length of the recovery was appropriate.

During our inspection, we uncovered multiple reasons and deficiencies that contributed to the website outage at NPS, DOI, and OIG. These included NPS information systems that—

- had not been properly authorized to operate;
- had outdated system inventories and were missing security documentation; and
- had insufficient contingency planning to prepare for a major power failure.

In addition, we found that no written agreements existed between NPS, DOI, and OIG describing the roles and responsibilities of each entity.

Background

NPS has over 400 locations throughout the United States whose interconnected networks and computer systems are known as the NPS One General Support System (One GSS). NPS has a web hosting and content management system in its Lakewood, CO, data center referred to as the Denver Data Center Child System (DDC) that manages the content for NPS' and DOI's websites. According to the DDC's system documentation, the DDC is a subsystem (child) of One GSS. NPS contracts with a Cloud-based content delivery network (CDN)² provider that delivers NPS and DOI web content to the public. Under a 2009 verbal agreement, NPS agreed to

¹The DDC hosts several other DOI websites, including, but not limited to, OIG, the Office of the Secretary, and the Office of the Solicitor. Most DOI bureaus, however, do not use NPS or DOI for web hosting services and were not affected by this outage. ²A CDN is an interconnected system of computers on the Internet that provides website content rapidly to numerous users by duplicating the content on multiple geographically distributed servers and directing the content to users based on proximity.

host the DOI website in the DDC and continuously maintain the content hosted by the CDN. After an extended outage of the OIG website in 2012, DOI's Office of Communications suggested that OIG allow DOI to host and manage the OIG website. OIG verbally accepted DOI's offer in 2012 to share web hosting and content management services, thus migrating OIG's website to DDC; NPS, however, was not informed of this decision.

On January 1, 2014, the DDC experienced a power outage that affected over 100 servers and, in some cases, caused physical damage. As a result of the outage, the DOI and OIG websites were unavailable between January 1 and January 7, 2014.

In response to the outage, on January 3, 2014, DOI uploaded a temporary web page to the CDN that contained links to the bureau websites unaffected by the outage. Although NPS hosts the OIG website, it does not host the OIG hotline web page; therefore, the hotline page was unaffected by the outage. DOI did not include a link to the hotline page on the temporary web page.

Findings

Our inspection revealed several concerns with DOI's web hosting services, including insufficient assessment and authorization processes and incomplete documentation, noncompliance with contingency planning and testing requirements, and no written documentation identifying the roles and responsibilities for shared services.

Insufficient Assessment and Authorization Processes and Incomplete Documentation

During our inspection, we could not determine whether the information systems hosting the NPS, DOI, and OIG websites were included in the One GSS assessment and authorization (A&A) boundary, as required by the Federal Information Security Management Act of 2002, because NPS did not have accurate system inventory documentation. In addition to incomplete system inventories for identified information system boundaries, we discovered insufficient contingency planning processes, an unauthorized information system, missing baseline configuration documentation, and a variety of other missing documentation.

An A&A boundary establishes the scope of protection for organizational information systems and includes the people, processes, and information technologies that are part of the system. Incomplete documentation of the One GSS boundary represents NPS' inadequate assessment of the system and the data the system hosts. As a result of insufficiently following A&A processes defined by Federal regulations and noncompliance with security documentation requirements (see Appendix 1), we cannot rely on the annual assurance statement that NPS signed supporting continuing authorization to operate for One GSS and the DDC.

According to the National Institute of Standards and Technology (NIST) every component of an information system must be a member of an identified information system boundary to obtain authorization to operate and that up-to-date system inventories, including identification of parent and child system relationships, are essential to providing authorizing officials an accurate and complete understanding of the system (see Appendix 1). We found that

the servers hosting the DOI and OIG websites appeared to be included in the system inventory of the DDC A&A boundary, but NPS did not clearly document the parent-child relationship between One GSS and the DDC. Although the DDC identified itself as a child of the One GSS information system boundary, One GSS did not identify the DDC as a child system. Therefore, One GSS did not include the DDC and its components in its system inventory. In addition, documentation for One GSS, including system and inventory documentation, was not kept up to date. As a result, NPS did not know that the DDC hosted the OIG website and therefore did not include it in the One GSS system inventory.

We also found that One GSS only inventories systems monitored with Microsoft System Center Configuration Manager (SCCM). SCCM, however, generates an incomplete system inventory for One GSS because it excludes all non-Microsoft components. NPS configured SCCM to inventory and manage only Microsoft computers and servers, but other documentation for the One GSS boundary indicated the existence of several non-Microsoft components, including network equipment, websites, and data types. According to NIST, a system inventory should include the entire environment of the operation, including all components of the information system. NPS only used data from SCCM as documentation for the One GSS inventory, making the One GSS inventory wholly incomplete.

In addition, we determined that the CDN had not been authorized to operate because NPS incorrectly believed that contractor systems were not required to be included within an information system boundary and undergo A&A. NIST and DOI criteria require that all systems, including contractor systems, operate through the A&A process (see Appendix 1). We also found that the CDN's baseline configuration for the DOI and OIG websites was set to refresh content every 6 hours, which is a short-lived setting in comparison to the 30-day refresh setting for the NPS website. Due to the power outage, the CDN could not communicate with the DDC during its refresh interval; the CDN interpreted the outage as an intentional update and purged the DOI website, which subsequently purged the OIG website. NPS reported that it had no baseline configuration documentation to identify why the 6-hour refresh for the DOI and OIG websites was set within the CDN.

Baseline configurations determine the security control selection process, but NPS could not provide us with baseline information for the CDN. Baselines provide a starting point for evaluating the overall risk of the information system and are established after the system owner and the owner's staff have formally reviewed and agreed upon them. Established baseline configurations and appropriate change control procedures facilitate the risk management process to identify and accept or mitigate the risks associated with deviating from that baseline. An appropriate A&A package for the CDN should have included a detailed description of system connections and data flow processes and may have alerted NPS to the risk associated with the short-lived baseline configuration for refreshing the content of the DOI and OIG websites.

Lastly, we could not determine which system security plan was authoritative for the DDC because NPS manually created, externally maintained, and uploaded its system security plan to the Cyber Security Assessment and Management (CSAM) tool instead of using the automated report generation capability. CSAM is a system used for managing A&A packages that has the capability to automatically create and make updates to the system security plan by incorporating

all of the latest system updates as input by the system owner. DOI regulations require all systems to use CSAM as the authoritative repository for all A&A documentation (see Appendix 1).

We identified several other required documents missing from CSAM, including—

- contingency plan test results;
- a continuous monitoring plan;
- a business impact assessment;
- a risk assessment report; and
- results from quarterly control assessments.

As a result of insufficient A&A processes and incomplete security documentation, NPS could not have effectively set priorities and managed risk according to the NPS, DOI, or OIG risk strategies. NPS officials could not have made a fully informed decision to grant authorization to operate to One GSS using the available information.

Noncompliance With Contingency Planning and Testing Requirements

NPS could have been better prepared to efficiently respond to and minimize damage and downtime from the outage if it had an appropriate contingency plan in place. NIST guidance requires bureaus and offices to test contingency plans annually (see Appendix 1). These plans help ensure adequate preparation to cope with the loss of operational capabilities due to a service disruption, such as an act of nature, fire, accident, or sabotage. According to NIST, these plans should cover all key functions, including assessing an agency's information technology and identifying resources, minimizing potential damage and interruption, developing and documenting the plan, and testing the plan and making necessary adjustments.

Our inspection found that the One GSS contingency plan had not been reviewed or updated since December 11, 2008. CSAM did not have contingency plan test documentation for the One GSS boundary, which indicates that the plan has never been tested. Contingency planning is another component of the risk management framework that establishes thorough plans, procedures, and technical measures that enable quick and effective system recovery following a service disruption.

NPS documentation stated that the DDC contingency plan has been tested annually as required, but we concluded that the tests conducted were inadequate. For example, the DDC test conducted on June 13, 2013, tested NPS' security incident response capability to an unauthorized user but not its capability to recover from an outage. Moreover, the DDC test conducted on January 10, 2012, tested the validity of the backups for restoring a single server, but the severity of the scenario did not trigger activation of the plan. Since neither test scenario activated the contingency plan, NPS had not conducted appropriate testing and was therefore unprepared to respond to the consequences of the outage.

We also determined that the DDC did not have adequate backup power for the number of servers, workstations, and routers it supports to minimize physical damage to equipment. The battery backup only lasted approximately 30 minutes, which was not enough time for NPS

personnel to power down the servers. NPS stated that it did not have a shutdown plan or an automated shutdown capability, which resulted in damage to multiple servers. Basic physical and environmental protections are required by NIST for the protection of equipment in information system boundaries such as One GSS and DDC (see Appendix 1).

No Written Documentation Identifying the Roles and Responsibilities for Shared Services

Lastly, we determined that NPS, DOI, and OIG do not have written agreements for website hosting, system ownership, support to contingency planning, recovery timeframes, or funding. NPS hosts the DOI website under a verbal agreement made in 2009 between individuals that no longer work for DOI, and DOI's Office of Communications does not know the terms of that agreement. In addition, in 2012, OIG verbally agreed to transfer the hosting and content management services of its website to DOI. Prior to this inspection, OIG did not know that NPS hosted either the DOI or OIG website.

Our inspection revealed that NPS and DOI disagree over ownership of the system boundary that covers DOI's website, ownership of the data, and the importance of the websites' availability to the public. The prevailing attitude of NPS officials appeared to indicate that a timely recovery of the DOI website was not their priority. Appropriate documentation, such as a memorandum of understanding or a service level agreement, that defined the roles and expectations for NPS, DOI, and OIG, would have alleviated disagreement among the three parties, and each entity would have had a clear understanding of its responsibilities related to web hosting and content management services, including the prioritization of system restoration in the event of a major outage.

Recommendations

We recommend that DOI's OCIO and Office of Communications:

- 1. Establish an oversight process to review and improve the effectiveness of A&A activities within DOI;
- 2. Establish a review process for determining the validity of annual assurance statements;
- 3. Establish an oversight process to enforce proper CSAM use for all systems;
- 4. Assess the risk of continuing to host DOI data at the DDC based on NPS' A&A activities; and
- 5. Document and approve appropriate service level requirements and operational and security role expectations for continued use of NPS' hosting services.

We recommend that NPS:

- 1. Perform an accurate A&A for the CDN, the DDC, and One GSS following all applicable laws, regulations, and requirements to continue to operate;
- 2. Establish a process to identify systems with inadequate A&A;
- 3. Upload all system documentation for all information systems, including the CDN, the DDC, and One GSS, to CSAM immediately after approval;
- 4. Establish a process to enforce proper CSAM use for all NPS systems;
- 5. Perform a new business impact analysis for both the DDC and One GSS based on customer data and recovery time objectives;
- 6. Update contingency plans incorporating customer recovery time objectives and expectations, accurate system inventories, and lessons learned from the recent outage;
- 7. Update the facility power capabilities or migrate the web hosting platform to a facility that meets physical and environmental requirements if NPS is required to meet customer recovery time objectives and expectations;
- 8. Design and conduct annual contingency plan tests; and
- 9. Document in writing and approve all agreements for providing web hosting services.

Please provide us with your written response to this report within 30 days. The response should provide information on actions taken or planned to address the recommendations, as well as target dates and title(s) of the official(s) responsible for implementation. Please send your response to:

Kimberly Elmore
Assistant Inspector General
Office of Audits, Inspections, and Evaluations
U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428
1849 C Street, NW.
Washington, DC 20240

Scope and Methodology

We focused our inspection on DOI, OIG, and NPS website hosting associated with the website outages in early January 2014. We reviewed the NPS services at the NPS data center in Lakewood, CO, and interviewed staff at DOI's Office of the Chief Information Officer, DOI's Office of Communications, NPS, and OIG. We also observed the physical environment at the NPS data center. Lastly, we reviewed Federal requirements for information systems and relevant

DOI, NPS, and OIG security documentation, policies, and procedures related to information security. We conducted this inspection in January 2014.

Although we included OIG data as part of the inspection sample, we conducted our inspection in accordance with the Quality Standards for Inspection and Evaluation as put forth by the Council of the Inspectors General on Integrity and Efficiency. We believe that the work performed provides a reasonable basis for our conclusions and recommendations.

OIG was not exposed to any undue influence during this assignment. Following our standard inspection procedures, OIG management was not involved in the daily activities of the inspection but did review and approve the working papers. The inspection team executed our internal procedures of indexing and referencing their findings, which involves linking the statements in the report to specific working papers and having an independent referencer verify the indexes to support all facts, figures, and findings. These review controls ensured that OIG remained independent and that the inspection was conducted in accordance with the Quality Standards.

The legislation creating the Office of Inspector General requires that we report to Congress semiannually on all audit, inspection, and evaluation reports issued; actions taken to implement our recommendations; and recommendations that have not been implemented.

If you have any questions regarding this report, please contact me at 202-208-5745.

cc: NPS Information Officer
DOI Office of Communications

Federal and Agency Policies and Procedures

Federal Law, Policy, Standards, and Guidance

- Federal Information Security Management Act of 2002 (FISMA): FISMA establishes the information security responsibilities of the head of each agency. This includes the responsibility for the security of any information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Under FISMA, the National Institute of Standards and Technology (NIST) is tasked with developing standards and guidelines. FISMA requires regular review and testing of all policies, procedures, and practices.
- Office of Management and Budget (OMB) Memo 11-33, "Fiscal Year 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management," September 14, 2011: OMB Memo 11-33 discusses the change from annual certification and accreditation to an ongoing risk-based approach to assessment and authorization (A&A) for ensuring the security of Federal information systems.
- OMB Memo 14-03, "Enhancing the Security of Federal Information and Information Systems," November 18, 2013: OMB Memo 14-03 establishes timelines for the requirement to migrate to the risk management framework and continuous monitoring model used for ongoing A&A.
- Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Categorization of Federal Information and Information Systems,"
 February 2004: Agencies first categorize their information and systems as required by FIPS 199. This helps to ensure that appropriate security requirements and security controls are applied to all Federal information and information systems including Cloud computing.
- FIPS Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006: After completing the categorization process in FIPS 199, agencies are then required to select an appropriate set of security controls from NIST Special Publication 800-53 to satisfy minimum security requirements. FIPS 200 and NIST Special Publication 800-53 help ensure that appropriate security requirements and security controls are applied to all Federal information and information systems. The assessment of risk determines the initial security control selection and determines if any additional controls are needed to protect organizational operations (including mission, functions, image, or reputation). The resulting set of required security controls establishes a level of security due diligence for the organization.
- NIST Special Publication 800-53 Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," August 2009, includes updates as of May 1, 2010: NIST Special Publication 800-53 defines all security controls applicable to Federal information systems and covers the steps in the risk management framework

that address security control selection. In this document, security controls related to 18 security control families are available for organizations to select when they undergo the FIPS 200 control selection process. Each security control family contains the specific security controls related to the security functionality of the family, including security assessment and authorization, contingency planning, physical and environmental protection, and risk assessment.

- NIST Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems," February 2010: The risk management framework (RMF) describes a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF defines an authorization boundary and states that all components of an information system be authorized for operation by an authorizing official. Initial authorization to operate is based on evidence available at one point in time, but systems and environments of operation change. Ongoing assessment of security control effectiveness supports a system's security A&A over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions and business processes. The RMF is the process for obtaining system authorization and, more generally, for managing and continually monitoring information security and information system-related risk.
- NIST Special Publication 800-137, "Information Security Continuous Monitoring for Federal Information Systems and Organizations," September 2011: NIST Special Publication 800-137 states that agencies must develop information security continuous monitoring (ISCM) activities that include multiple tiers of an organization. There are different responsibilities for each tier in order for a system to obtain authorization to operate and each tier must continually monitor security controls to maintain that authorization. The ISCM process must also include organizationally determined assessment and monitoring frequencies. Through ISCM, new threat or vulnerability information is evaluated as it becomes available, permitting organizations to make adjustments to security requirements or individual controls as needed to maintain authorization decisions.

DOI Policy and Guidance

- Office of the Chief Information Officer (OCIO) Directive 2011-006, "Information System Boundary Assessment & Authorization Package Documentation and Inventory," March 23, 2011: OCIO Directive 2011-006 establishes Cyber Security Assessment and Management (CSAM) as the official repository for all A&A documentation and provides instructions to bureaus for the proper use of the system. It also provides detailed guidance on how to establish information system and subsystem boundary relationships between general support systems, major applications, and minor applications.
- OCIO Memorandum 0000228, "Ongoing Assessment and Authorization Through Continuous Monitoring," March 16, 2012: CIO 0000228 redefines the certification and

accreditation guidance to be called the A&A process and requires the implementation of the risk management framework and continuous monitoring instead of conducting annual reauthorizations.

• OCIO Memorandum, "Contractor Systems," September 30, 2013: The OCIO contractor systems memorandum provides a clear definition of each type of contractor system and provides clarification to bureaus that all contractor systems must also obtain authority to operate through the A&A process.

Report Fraud, Waste, and Mismanagement



Fraud, waste, and mismanagement in Government concern everyone: Office of Inspector General staff, departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Internet: www.doi.gov/oig/index.cfm

By Phone: 24-Hour Toll Free: 800-424-5081

Washington Metro Area: 202-208-5300

By Fax: 703-487-5402

By Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 4428 MIB 1849 C Street, NW. Washington, DC 20240



U.S. Department of the Interior Office of Inspector General

Evaluation Report

THE DEPARTMENT OF THE INTERIOR'S PROCESS TO MANAGE INFORMATION TECHNOLOGY SECURITY WEAKNESSES



United States Department of the Interior

Office of Inspector General Washington, D.C 20240

SEP 23 2005

Memorandum

To:

Assistant Secretary for Policy, Management and Budget

From:

Earl E. Devaney

Inspector General

Subject:

Department of the Interior's Process to Manage Information Security

Weaknesses (Report No. A-EV-MOA-0001-2005)

The attached report presents the results of our evaluation of the Department's process to manage information technology security weaknesses. We concluded that the Department had not implemented an effective plan of actions and milestones (POA&M) process and as a result, the process should be reported as a material weakness under the Federal Managers' Financial Integrity Act of 1982 in the 2005 Performance and Accountability Report. Our report presents recommendations that are designed to assist the Department in improving its POA&M process.

In the September 14, 2005 response to the draft report, the Department's Chief Information Officer did not specifically concur or non-concur with our findings and recommendations. The response indicated that the Department had fully implemented three of the five recommendations and that no further action was needed to implement the remaining two recommendations. Although we acknowledge recent steps taken by the Department to improve the POA&M process, the actions taken have not fully addressed our recommendations. Accordingly, we consider all five recommendations unresolved.

To resolve the report, we would appreciate your specific comments on actions taken or planned, including target dates and titles of responsible officials, to implement the recommendations. Therefore, as required by Departmental Manual (360 DM), please provide us with your written response to the report by October 23, 2005.

The legislation, as amended, creating the Office of Inspector General requires that we report to Congress semiannually on all audit reports issued, actions taken to implement our recommendations, and recommendations that have not been implemented.

We appreciate the cooperation provided by the Department and agency staff during our evaluation. If you have any questions regarding this report, please call me at (202) 208-5745.

Attachment

EXECUTIVE SUMMARY

WHY WE DID THIS EVALUATION

The Office of Management and Budget (OMB) requires federal agencies to maintain a plan of action and milestones (POA&M) to assist in identifying, assessing, prioritizing, and monitoring progress to correct information technology security weaknesses found in systems and programs. The POA&M is also used to report progress on remediation efforts to correct security weaknesses to OMB and Congress. The Department of the Interior's (Department) Chief Information Officer (CIO) has stated that the POA&M is the Department's authoritative tool for managing information technology (IT) security weaknesses. The objective of our evaluation was to determine whether the Department's POA&M process was adequate.

RESULTS IN BRIEF

We found that the Department had not implemented an effective POA&M process. Specifically, our evaluation determined that the Department's POA&M:

- did not contain all known weaknesses;
- included weaknesses reported as corrected which in fact were not corrected; and
- insufficiently described weaknesses and planned corrective actions.

These problems occurred because the Department's Office of the CIO had not instituted effective quality assurance and verification processes to ensure that bureaus and offices reported complete, accurate, and reliable information. The process, as implemented, did not hold responsible officials accountable for reporting accurate and reliable information in the POA&M. Further, the process did not require weaknesses be prioritized on a Departmental basis. Additionally, the automated system used for the Departmental POA&M did not contain standardized information or provide for easy information queries or reporting, which limited its usefulness as a management tool.

As a result, the Department lacks assurance that the most critical security weaknesses are being corrected first and that its systems and data are adequately safeguarded. Furthermore, the Department is reporting inaccurate and misleading information to OMB and Congress.

In our opinion, the POA&M process should be reported as a material weakness under the Federal Managers' Financial Integrity Act of 1982 in the Department's 2005 Performance and Accountability Report.

To improve the Department's POA&M process, we recommend that all identified IT security weaknesses be reported and prioritized; the status of corrective actions be

monitored and verified; and responsible officials be held accountable for the accuracy of their data in the POA&M. Additionally, we are recommending that the Department upgrade its automated system to be a useful management tool.

TABLE OF CONTENTS

INTROL	OUCTION	·• I
Ва	ckground	1
	ior Reviews	
	ojective and Scope	
RESULT	TS OF EVALUATION	3
De	epartment's POA&M Was Not Reliable	3
	anagement Oversight Was Not Effective	
	ne Department Lacks Assurance Its IT Systems Are Secure	
RECOM	MENDATIONS, DEPARTMENT OF THE INTERIOR'S CHIEF	
	MATION OFFICER REPLY, AND OFFICE OF INSPECTOR	
•		
	•	10
	AL REPLY	10
	AL REPLY	10
GENER Appeni	AL REPLY	10
GENER Appeni	AL REPLY	10
GENER Appeni	OICES Office of Inspector General Prior Reports with Findings	
GENER APPENI 1.	OICES Office of Inspector General Prior Reports with Findings Related to the Department of the Interior's Plan of Action	.16
GENER APPENI 1. 2.	OICES Office of Inspector General Prior Reports with Findings Related to the Department of the Interior's Plan of Action and Milestones	.16
GENER APPENI 1. 2.	OICES Office of Inspector General Prior Reports with Findings Related to the Department of the Interior's Plan of Action and Milestones Scope, Methodology, and Criteria Summary Results of Weaknesses Tested from Bureaus'	.16
GENER APPENI 1. 2.	OICES Office of Inspector General Prior Reports with Findings Related to the Department of the Interior's Plan of Action and Milestones Scope, Methodology, and Criteria	.16
GENER APPENI 1. 2. 3.	OICES Office of Inspector General Prior Reports with Findings Related to the Department of the Interior's Plan of Action and Milestones Scope, Methodology, and Criteria Summary Results of Weaknesses Tested from Bureaus' Plans of Actions and Milestones, September 15, 2004 and December 15, 2004	.16 .18
GENER APPENI 1. 2. 3.	OICES Office of Inspector General Prior Reports with Findings Related to the Department of the Interior's Plan of Action and Milestones	.16 .18
GENER APPENI 1. 2. 3.	Office of Inspector General Prior Reports with Findings Related to the Department of the Interior's Plan of Action and Milestones	.16 .18
GENER APPENI 1. 2. 3.	Office of Inspector General Prior Reports with Findings Related to the Department of the Interior's Plan of Action and Milestones Scope, Methodology, and Criteria Summary Results of Weaknesses Tested from Bureaus' Plans of Actions and Milestones, September 15, 2004 and December 15, 2004 POA&M Practices and Automated System Capabilities From Department of the Interior Bureaus and the Environmental Protection Agency	.16 .18
GENER APPENI 1. 2. 3. 4.	Office of Inspector General Prior Reports with Findings Related to the Department of the Interior's Plan of Action and Milestones	.16 .18 .21

ACRONYMS AND TERMS

BLM Bureau of Land Management

BOR Bureau of Reclamation

bureau Department of the Interior's bureaus and offices

CIO Chief Information Officer
Department Department of the Interior

FISMA Federal Information Security Management Act of 2002

GS Geological Survey IA Indian Affairs

IT Information technology

MMS Minerals Management Service

NPS National Park Service

OIG Office of Inspector General

OMB Office of Management and Budget

OS Office of the Secretary

POA&M Plan of action and milestones

INTRODUCTION

BACKGROUND

A plan of action and milestones is used to identify, assess, prioritize, and monitor the progress of corrective efforts regarding information technology security weaknesses identified in a system or a program.

The Federal Information Security Management Act of 2002 (FISMA) requires federal executive branch agencies to develop a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices of the agency. The Office of Management and Budget (OMB) designed¹ the plan of action and milestones (POA&M) to meet this requirement.

OMB policy requires a POA&M be prepared for each system and program where information technology (IT) security weaknesses have been found. A POA&M should identify each weakness including the related corrective actions, the scheduled completion date for correcting each weakness, and the status for correcting each weakness. The Department of the Interior's (Department) bureaus and offices (bureaus) should prepare POA&Ms for each of their systems and programs where security weaknesses have been identified. The Department's Office of the Chief Information Officer (CIO), using the bureaus' data, prepares a POA&M for the Department that is submitted to OMB. In the Department's September 15, 2004 POA&M, the Department reported that it had 157 IT systems and 13 programs, that there were 2,243 IT security weaknesses, and that 883 of these 2,243 weaknesses had been corrected. The Department also reported that it would cost approximately \$125 million to correct the total 2,243 weaknesses (including the funds already spent to correct the 883 weaknesses).

PRIOR REVIEWS

The Government Accountability Office has not issued any reports related to the specific objective of this evaluation. The Office of Inspector General (OIG) has issued three reports on the Department's information security program that included findings related to the Department's POA&M process. (See Appendix 1 for summaries of these findings.) In the most recent report, *Annual Evaluation of the Information Security Program of the Department of the Interior* (Report No. A-EV-MOA-0006-2004), we noted that the Department had established a POA&M process consistent with OMB guidance. However, the evaluation was limited and did not include tests to determine

¹ OMB Memorandum M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," issued October 17, 2001. This Guidance was updated by OMB Memorandum M-03-19, "Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting."

whether the process was properly implemented. In that same report, we concluded that all weaknesses were not recorded in the POA&M, priorities were not assigned to correct all weaknesses, and costs for actions to remedy weaknesses were not always identified.

OBJECTIVE AND SCOPE

The objective of our evaluation was to determine whether the Department's POA&M process to manage IT security weaknesses was adequate. To accomplish our objective, we interviewed personnel involved with the process, analyzed the Department's POA&Ms of September 15 and December 15, 2004, and conducted tests of weaknesses reported as corrected. In performing our tests, we judgmentally selected 133 weaknesses in 20 IT systems and 1 security program. These systems and program were owned by the Office of the Secretary (OS), the Assistant Secretary of Indian Affairs (IA), the Bureau of Land Management (BLM), the Bureau of Reclamation (BOR), the Geological Survey (GS), the Minerals Management Service (MMS), and the National Park Service (NPS). (See Appendix 2 for more details on scope, methodology, and the criteria used in this evaluation.)

RESULTS OF EVALUATION

DEPARTMENT'S POA&M WAS NOT RELIABLE

We concluded that the Department's POA&M could not be used to effectively manage the Department's IT security weakness remediation process. The POA&M was incomplete, inaccurate, and misleading.

Known Weaknesses Were Not Reported

We found that not all known weaknesses were included in the Department's POA&M. For example, bureau staff indicated that:

- unless a weakness was determined to be "material" it would not be reported (GS and NPS).
- weaknesses were not reported (1) when identified through day-to-day operations, (2) which could be corrected within short time frames, or (3) when the security risks were determined to be low and accepted by levels of management at or below bureau IT system owners (OS, IA, BOR, GS, and NPS).

In addition, we found that the Department did not have POA&Ms in place for 11 systems that were not yet certified and accredited. Lack of certification and accreditation is a known weakness that must be addressed and should be documented in a POA&M.

Weaknesses Reported as Corrected Were Not Corrected

About half (64 of 133) of the weaknesses reported as corrected which we tested were not corrected. (See Appendix 3 for a summary of the results of the IT security weaknesses we tested.) Specifically, we determined that corrective actions were either not performed or were not sufficient to correct weaknesses. For example,

- ➤ Three corrective actions required the purchase of computer equipment, but the equipment had not been ordered.
- ➤ Nine corrective actions required that contingency plans be developed, tested, and updated, but the plans were nonexistent, were still in draft, or had not been updated.

- > Five corrective actions required a new IT system be implemented, but the system had not been implemented.
- Seven corrective actions required the issuance of policies, but the policies issued did not adequately address the weaknesses.
- ➤ Fourteen corrective actions required that management accept the security risks associated with the weaknesses. However, the documentation supporting managements' acceptance of risk was nonexistent, did not adequately justify risk acceptance, or was not created until after our request for the documentation.

Descriptions of Weaknesses and Actions to Correct Weaknesses Were Not Adequate

In our analysis of the information reported in the Department's POA&M, we also found that weaknesses and actions to correct weaknesses were not always adequately described. Weakness descriptions such as "data integrity," "user passwords cracked," and "insufficient auditing capability" were used. For example, in a weakness described as "insufficient auditing capability" the planned corrective action was to "implement controls for sufficient auditing capability." We believe that these descriptions did not clearly convey the significance of the weakness being reported or what specific actions were planned to correct the weakness.

MANAGEMENT OVERSIGHT WAS NOT EFFECTIVE

The Department's Office of the CIO had issued some policies and procedures regarding the POA&M process. However, the Office did not oversee the process to ensure that the Department's POA&M could be used to effectively manage IT security weakness remediation and was accurate, timely, and resulted in safeguarding IT resources. Specifically, the Office of the CIO did not institute adequate quality assurance and verification methodologies and did not require that responsible officials, such as bureau heads, be accountable for the accuracy of reported information and for correcting IT security weaknesses. The Department's CIO also had not instituted an effective process to ensure that weaknesses were prioritized based on the risk to the Department. In addition, the Department's Office of the CIO had not ensured that the automated system used for the POA&M could be used as an effective management tool.

No Quality Assurance Process

The Office of the CIO had not established an effective quality assurance process to review information submitted in the bureaus' quarterly POA&Ms to ensure accurate and complete information was included in the Department's POA&M. Although the Office of the CIO performed a limited review of the count of weaknesses reported by the bureaus, this review was not comprehensive and did not ensure that (1) all systems in the Department's IT system inventory were included; (2) IT security weaknesses were clearly described so that weaknesses were understood; and (3) reported planned corrective actions would correct the weaknesses. For example, the Department's September 15, 2004 POA&M:

- ➤ Did not include an Office of Surface Mining Reclamation and Enforcement (OSM) system. This happened because OSM did not include the system in its quarterly submission to the Department and the Department did not compare OSM's submission to the Department's IT system inventory to ensure completeness.
- ➤ Included more than 300 vague or incomplete IT security weakness descriptions. These vague descriptions included nine U.S. Fish and Wildlife Service (FWS) weaknesses of "contingency plans," four BOR weaknesses of "insufficient auditing," and an MMS and an NPS weakness of "auditing." The Department did not request clarification from the bureaus for vague descriptions.
- ➤ Included approximately 700 IT security weaknesses that did not have sufficient planned actions that would correct the respective weaknesses. For these weaknesses, all of the bureaus reported that only one corrective action was planned, such as to implement a policy but did not include information describing how the policy would be implemented. For example, a BLM IT security weakness was described as the lack of separation of duties among security and administration personnel. The planned corrective action did not identify what would be done to separate the duties. Rather, the only planned corrective action was to report the weakness to a CIO Council. The Department did not require bureaus to clarify planned corrective actions.

Without a quality assurance process, the Department's CIO is not able to improve the quality and reliability of the Department's POA&M and the Department cannot ensure that its POA&M process is effective.

No Verification Process

We found that the CIO relied on bureaus to develop and maintain the documentation supporting corrected weaknesses and did not have a process to verify that actions were taken as reported. When we reviewed bureau procedures, we found that bureau IT security weaknesses were often considered corrected based on individuals stating they had corrected the weaknesses. The bureaus did not verify that weaknesses were corrected or that documentation, such as a cost benefit analysis had been prepared to support acceptance of risk. Therefore, the Department's September 15, 2004 POA&M inaccurately reported that weaknesses were corrected. Further, this process did not prevent IT security risks from being accepted inappropriately. For example:

- MMS had reported that 15 security weaknesses for one of its systems had been corrected; however, in our tests of the 15 reportedly corrected weaknesses, no supporting documentation existed to demonstrate that the corrective actions were implemented and tested. Further, we determined that 8 of these weaknesses had not been corrected.
- ➤ BOR reported that a security weakness for one of its IT systems was "insufficient user access controls." BOR reported that the weakness would not be corrected because "management accepted risk." BOR planned to accept the risk because (1) there were limited controls available in the system and (2) BOR would limit the number of users with direct access to the system through Rules of Behavior and oversight.

BOR's documentation was not sufficient to support the acceptance of the risk because it did not include information such as a cost-benefit analysis or an adequate description of the planned mitigating controls such as oversight. The documentation also did not identify the position and title of the individual deciding to accept the risk.

Without a verification process, the Department has little assurance that its IT security weakness remediation process is effective. Appendix 4 describes good bureau practices that we believe could also be used by the Department as part of a verification process.

Inappropriate Accountability for Accurate Information in POA&Ms

Bureau heads and bureau IT system owners were not accountable for true and accurate security weakness information. Instead the Department CIO had established inappropriate accountability for reporting accurate and reliable information in the bureaus' POA&Ms. The responsibility was placed on organizations that originally identified the weakness, which could include the OIG or contractors. For example, we were told by the IA's Deputy for IT Security and Privacy that its contractors' were responsible for accurate IT security weakness descriptions in IA's POA&Ms. Neither the OIG nor contractors should be responsible for the accuracy of the Department's and bureaus' POA&M data. We believe that accountability should be established through a certification process where appropriate bureau officials, such as bureau heads, certify that POA&M information is accurate.

Weaknesses Were Not Prioritized Departmentwide

The Department's POA&M process required that weaknesses be prioritized only at the bureau level rather than Departmentwide. That is, the Department CIO did not always intervene in the prioritization of IT security weaknesses to ensure that the most critical weaknesses to the Department's mission and goals were corrected first. Consequently, we found that medium priority weaknesses for less critical systems were being corrected before high priority weaknesses for more critical systems. For example, two medium priority security weaknesses in an Office of the Secretary business essential IT system were corrected before two high priority security weaknesses of an MMS mission critical IT system.

Automated POA&M Information System Not Effective

Bureau staff indicated that the Department's automated POA&M system was difficult to use and that usable information could not be produced. The Department's automated POA&M system could not be used to monitor, prioritize, and report on IT security weaknesses. For example, the Department's automated system, as it was implemented, does not:

- contain standardized descriptions of weaknesses and related corrective actions so that the Department could accurately prioritize all the weaknesses;
- allow for monitoring the status of specific weaknesses without extensive searching through the system;
- allow for querying information for management purposes; or
- produce a report that could be submitted to OMB without extensive editing.

Because of deficiencies in the current automated POA&M system, one bureau implemented its own system and other bureaus manually prepare their POA&M information. Generally, bureau system personnel gather and organize the information for weaknesses related to their IT systems based on bureau practices. The system personnel then submit the information to the bureau POA&M coordinator who compiles the POA&M information for all of the bureau's systems. Each bureau then submits its POA&M information to the Department. The Department must manually compile this information on approximately 2,200 weaknesses with about 2,900 corrective actions from at least 170 IT systems and programs. This compilation process begins almost 2 months before the information is sent to OMB and is repeated by the bureaus and the Department on a quarterly basis. This is not cost effective for the Department and needs to be addressed before each bureau implements its own automated system. In Appendix 4, we describe capabilities we found in reviewing POA&M automated tools at IA and the Environmental Protection Agency that the Department could use to improve its POA&M system.

THE DEPARTMENT LACKS ASSURANCE ITS IT SYSTEMS ARE SECURE The Department's CIO has stated that the POA&M is the Department's tool to manage IT security weaknesses. As such, the Department is relying on information that we found to be inaccurate, incomplete, and untimely. Without reliable information in the POA&M, the Department cannot identify

systemic problems and monitor corrective actions. Also, management may make inappropriate decisions regarding the Department's information security program. Therefore, the Department cannot ensure that the most significant weaknesses are corrected first and that its systems and data are adequately safeguarded.

If the Department does not correct its process, it will continue to provide inaccurate and incomplete information to OMB and Congress. The Department should report this condition as a material weakness under the Federal Managers' Financial Integrity Act of 1982 in the Department's 2005 Performance and Accountability Report.

RECOMMENDATIONS, DEPARTMENT OF THE INTERIOR'S CHIEF INFORMATION OFFICER RESPONSE, AND OFFICE OF INSPECTOR GENERAL REPLY

In the September 14, 2005 response, the Department's Chief Information Officer (CIO) did not specifically concur or non-concur with our findings and recommendations. The response indicated that the Department had fully implemented recommendations 1, 2, and 3, and that no further action was needed to implement recommendations 4 and 5. Overall, the CIO stated that it had addressed all recommendations, eliminating any need to elevate concerns to the level of material weakness for this fiscal year.

Although we acknowledge recent steps taken by the Office of the Chief Information Officer (OCIO) to improve the POA&M process, we continue to believe that the current process needs to be improved and that the POA&M process should still be reported as a material weakness. Based on the CIO response, we consider all five recommendations unresolved.

We recommend that the Department Chief Information Officer, considering the bureau and the Environmental Protection Agency promising practices in Appendix 4:

Recommendation 1

Institute a quality assurance process to ensure:

- a. all weaknesses are reported.
- b. weaknesses are completely described and the respective corrective actions would adequately correct the weaknesses. This could be partially addressed through establishing standardized descriptions of common weaknesses and related corrective actions.

DOI Response

The Department described additional quality assurance processes in place as a result of our evaluation that it believes fully implements this recommendation. Specifically,

 The Department issued guidance requiring "Each IT security weakness identified in any review of a program or system must be entered on the authoritative POA&M..."

- The Department initiated a quality assurance process through OCIO Directive 2005-007 dated May 3, 2005 in which the Department stated that all bureaus complied. The Department refined and clarified its procedures in an August 18, 2005 memorandum. Additional guidance in a new OCIO Directive and POA&M Process Standard for implementation in FY 2006 will further enhance the POA&M processes.
- The Department also noted that OMB 04-25 does not require sensitive weakness descriptions, but endorses the use of general or brief descriptions. Separate source documents and reports should detail more fully information provided in the POA&M.

OIG Reply

The Department has taken recent steps to improve the POA&M process including the issuance of more detailed guidance. However, we believe that further steps are needed to implement an effective quality assurance process. While the recent guidance communicates the requirement to include all weaknesses in the POA&M, it does not describe a Department level quality assurance process to ensure that all weaknesses are actually reported. The working draft Plan of Actions and Milestones Process Standard does state that the Department Chief Information Officer (CIO) and the Chief Information Security Officer (CISO) will be required to review the POA&Ms to ensure compliance with policies and procedures. The CISO will also be responsible for instituting a quality assurance process to ensure all systems are accounted for, weaknesses are adequately described, and corrective action plans appropriately address the weakness. However, these Standards will not be implemented until fiscal year 2006.

We agree that OMB M 04-25 endorses the use of brief descriptions and found that the OMB examples provided enough detail to understand the weakness. However, in our evaluation we identified weakness descriptions that did not meet OMB requirements. A quality assurance process would ensure weakness descriptions are adequate.

We consider this recommendation unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.

Recommendation 2

Institute a verification process to ensure that weaknesses reported as corrected are, in fact, corrected; that supporting documentation is maintained; and that management's acceptance of risk is appropriately justified and documented.

DOI Response

The Department described an additional quality assurance process and verification process that it has put in place as a result of our evaluation that they believe fully implements this recommendation. The Department specifically cites OCIO Directive 2005-007 with which it states that all bureaus complied. The bureaus and offices provided verifications that weaknesses that were reported as corrected were in fact corrected. The Department plans to issue an additional Directive and POA&M Process Standard for implementation in 2006 to provide further process guidance. The POA&M Process Standard will provide for an additional quality assurance process, to be performed by the OCIO, which will include inspection and review of a sample set of completed POA&M corrective actions each fiscal year. The Department also stated that it is not cost effective to complete a cost-benefit analysis for every security weakness in which the risk is accepted.

OIG Reply

The Department has taken some steps to improve the verification process including the requirement that the bureaus conduct verifications that the weaknesses reported as corrected were in fact corrected. However, the continued reliance on self reporting by the bureaus makes compliance verification virtually impossible from a Department-wide management standpoint. In its response, the Department indicated that the Plan of Actions and Milestones Process Standard would provide for an additional quality assurance to be performed by the OCIO which will include an "inspection and review of a sample set of completed POA&M corrective actions each fiscal year." However, the current draft does not include this additional process. The Department will not have an effective POA&M process until these verification reviews are established and implemented. Additionally, we included the cost benefit analysis in our report as a promising practice that could be used by the Department in its POA&M process.

We consider this recommendation unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.

Recommendation 3

Require senior bureau management to certify that information in the bureaus' POA&Ms is accurate and true. In the certification, bureau management should acknowledge that each POA&M includes all known weaknesses, that weaknesses are adequately described, that corrective actions would adequately correct the weaknesses, and that completed actions are in fact completed."

DOI Response

The Department responded that the quality assurance and verification process initiated by the OCIO Directive 2005-007 and further clarified in a memorandum dated August 18, 2005 requires senior management officials to ensure and verify information in the bureau's POA&M is accurate. The Department believes the implementation of the verification process fully implements this recommendation.

OIG Reply

The Department requires that remediation actions be certified by the applicable system owner and documented. We received certification statements for some of the bureaus' system POA&Ms. The certification statements only certified the completion of corrective actions to correct weaknesses, it does not certify that all known weaknesses are reported and that all required milestone tasks are included. Our recommendation was intended to require bureau officials to certify the **entire** POA&M and not just those weaknesses that were completed. We revised our recommendation accordingly.

Based on the Department response, we conclude that this recommendation is unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.

Recommendation 4

Institute a practice to review all Department IT system and program weaknesses to ensure the most critical weaknesses for the most critical systems of the Department are being addressed first.

DOI Response

The Department did not agree with this recommendation. The Department stated that the IT budget is under the authority of multiple appropriations and with specific restrictions on the movement of appropriated funds. Thus, prioritization across bureaus is not a relevant issue. Additionally, the Department makes the following points:

• NIST SP 800-57 requires the Designated Approving Authority (DAA) to make the final decision and be held accountable for accepting risks to their systems. Having higher levels of management make changes to the

DAA's determination would undermine the DAA's authority and accountability.

- Interior prioritizes corrective actions as indicated by the "Scheduled Completion Date" column.
- Sequential prioritization based on risk level alone does not make sense in an operational and budgetary context where some weaknesses are more easily and quickly corrected than others. Adhering to a strictly sequential work-off plan could leave a larger number of weaknesses unresolved, which could increase the overall risks to individual systems, potentially raising the system risk to unacceptable levels.

OIG Reply

We recognize that there are budgetary restrictions prohibiting movement of funds between bureaus in most cases. However, we were made aware that the Department has available funds to address certification and accreditation of bureau and office systems. The Department can use the POA&M as a management tool in setting priorities for allocating these funds Department-wide and ensuring the most critical weaknesses for the most critical systems are being addressed first.

Based on the Department response, we conclude that this recommendation is unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.

Recommendation 5

Implement an effective automated POA&M system. This can be accomplished by either improving the current system or implementing a new system. In establishing an effective system, the Department should define the requirements based on consultation with bureaus' IT operational staff, system owners, program managers, and others that are involved with the IT security weakness remediation process and canvass other federal agencies for best practices.

DOI Response

The Department recognizes the benefits of using POA&M automation tools and plans to evaluate tools for prospective use in the Department. They may not be able to immediately implement the recommendation or find it cost effective to do so. The Department believes that the current POA&M reporting format, while not optimal, meets basic requirements. A new automated POA&M system could not be funded until fiscal year 2008. The Department stated that the implementation of a single-purpose system for POA&Ms would not be beneficial because the functional requirements, such as automation of forms and workflow, are common to other Departmental and OCIO processes. Those requirements should be met with common software service components.

OIG Reply

The Department already has an automated POA&M system. Our review identified numerous deficiencies which resulted in one bureau purchasing and implementing its own system and other bureaus manually preparing their POA&M information. This is not cost effective for the Department. Our recommendation was intended to encourage the Department to improve its automated system to prevent the need for bureaus to manually prepare the information and allow for a unified Departmental process. This can be accomplished through either improving the current system or the implementation of a replacement system. In making its decision, the Department should take into consideration best practices used within the bureaus and by other federal agencies. We revised our recommendation to focus on the Department's need to identify the requirements of an effective POA&M system.

Based on the Department response, we conclude that this recommendation is unresolved. We are requesting that the Department reconsider the recommendation and provide the information requested in Appendix 6.

OFFICE OF INSPECTOR GENERAL PRIOR REPORTS WITH FINDINGS RELATED TO THE DEPARTMENT OF THE INTERIOR'S PLAN OF ACTION AND MILESTONES

REPORTS	FINDINGS	SUGGESTED IMPROVEMENTS AND RECOMMENDATIONS
ANNUAL EVALUATION OF THE SECURITY PROGRAM AND PRACTICES OVER NON-NATIONAL SECURITY SYSTEMS, U.S. DEPARTMENT OF THE INTERIOR (Report No. 2002-I-0049)	We noted the following deficiencies in the Department of the Interior's (Department) and the bureaus' and offices' (bureaus) July 31, 2002 plans of action and milestones (POA&Ms) to correct information technology (IT) security weaknesses: • Specific weaknesses were grouped. together as overall general weaknesses. • System weaknesses were rolled into one weakness and incremental steps to address the specific system weaknesses were not included. • Only a final completion date was given for corrective actions that involved multiple years. Incremental milestone dates had not been established to effectively measure progress. • Milestone dates or resources required to accomplish corrective actions were not always presented.	 Hold program officials accountable for carrying out their information security responsibilities. Hold subordinates of bureau heads accountable for fulfilling their information security responsibilities. Establish a process to validate that all bureaus have effectively implemented federal and Department security policies and procedures, standards, and guidelines for all systems. Include in the POA&Ms all necessary steps and specific completion dates.
ANNUAL EVALUATION OF THE INFORMATION SECURITY PROGRAM OF THE DEPARTMENT OF THE INTERIOR (Report No. 2003-I-0066)	Overall, POA&Ms developed by bureaus were not complete or used effectively. Specifically, the POA&Ms did not: Include all IT systems owned and operated by the Department that had weaknesses. Include all weaknesses whether identified through the organization's internal reviews or by organizations such as the Office of Inspector General. Include incremental steps for correcting weaknesses especially when milestone dates were in excess of 6 months. Always include costs for correcting weaknesses. Prioritize weaknesses in order of significance. Also, costs identified in the POA&Ms to correct security weaknesses were not always included in bureau capital investment plans.	 Include tests to validate that information reported by bureaus is adequate and that controls are operating as planned or intended in the Chief Information Officer's (CIO) information security program reviews of bureaus. Require that POA&Ms contain detailed steps for correcting reported weaknesses when the milestone dates exceed 6 months. Ensure that POA&Ms include all costs necessary to correct reported weaknesses, establish priorities, and integrate costs into the IT investment plans. Require each bureau to present to the CIO a strategic plan with incremental steps to achieve an institutionalized information security program that meets the requirements of the Federal Information Security Management Act (FISMA). The

REPORTS	FINDINGS	SUGGESTED IMPROVEMENTS AND RECOMMENDATIONS
		strategic plan should encompass the corrective actions in the POA&Ms and should be approved by the CIO.
ANNUAL EVALUATION OF THE INFORMATION SECURITY PROGRAM OF THE DEPARTMENT OF THE INTERIOR (Report No. A-EV-MOA-0006-2004)	The Department established a POA&M process consistent with Office of Management and Budget (OMB) guidance. We found that bureaus recorded known weaknesses in their POA&Ms most of the time. However, we also found a need to ensure that all weaknesses are reported, priorities are assigned to correct all weaknesses, and costs of actions needed to remedy weaknesses are always identified. Specifically, we found: • Agreed-upon weaknesses identified during Office of Inspector General (OIG) audits of bureau financial statements were not always included in the POA&Ms. • Bureaus did not incorporate all weaknesses identified through risk assessments and security tests and evaluations into their POA&Ms. • Remediation activities were not prioritized in the POA&Ms. • Resources were not always allocated based on prioritization of the weaknesses. • Resources required to complete remedial actions were not tied to budget documents. • POA&Ms did not include all of the weaknesses in a system.	The Department CIO should institute an oversight process to ensure bureaus effectively implement the Department's security program requirements. Specifically, the CIO must ensure that: • POA&Ms not only reflect prioritization of weaknesses but also identify the resources necessary to address the higher prioritized weaknesses so that the corrections of high priority weaknesses are performed first; • budget documentation and POA&Ms can be directly correlated through OMB project/system identifiers to ensure funding addresses security weaknesses; and • weaknesses identified during OIG and other internal or external reviews are included in the applicable POA&Ms at the time the weaknesses are identified and agreed to by the bureau.

Appendix 2

SCOPE, METHODOLOGY, AND CRITERIA

We conducted our evaluation in accordance with the *Quality Standards for Inspections* issued by the President's Council on Integrity and Efficiency. Our review was conducted from November 2004 through April 2005. To accomplish our objective, we:

- interviewed Department of the Interior (Department) and bureau and office (bureau) personnel involved in the plan of action and milestones (POA&M) process, including Chief Information Officers (CIO), information technology (IT) security managers, POA&M coordinators, and IT staff;
- reviewed the Department's and the bureaus' policies and procedures related to reporting IT security weaknesses and remediation activities on the POA&Ms;
- ➤ analyzed bureaus' IT systems and program quarterly POA&Ms that were submitted to the Department and the Department's quarterly POA&Ms that were submitted to the Office of Management and Budget (OMB) dated September 15 and December 15, 2004;
- ➤ identified practices within the Department and at other federal agencies to determine if methodologies are available to the Department for improving its POA&M reporting and remediation processes.

We also conducted tests of corrective actions for weaknesses reported as corrected in the POA&Ms. The Department's September 15, 2004 POA&M reported 157 IT systems and 13 programs with a total of 883 corrected weaknesses. The bureaus had reported to the Department for the same period 173 systems and 13 programs with 923 corrected weaknesses. We chose to select our sample from the bureaus' POA&Ms because these contained more detail. From the universe of 923 reportedly corrected weaknesses, we judgmentally selected weaknesses to test using the following methodology:

- ➤ We excluded financial and financial-related applications because the respective weaknesses are subject to review during the annual financial statements audits.
- ➤ We chose weaknesses that were related to access controls because of the significance of these controls in safeguarding IT resources and data and because these controls are included in most types of IT systems.

Based on this methodology, we identified an initial universe of 139 reportedly corrected IT security weaknesses for 39 IT systems and 1 program. Next we judgmentally selected 39 weaknesses in 18 systems and 1 program to test. We expanded our testing to include other weaknesses reported as corrected in the bureaus' POA&Ms of September 15 and December 15, 2004, for 6 of the 18 systems selected. We also included two additional IT systems with corrected weaknesses owned by the Office of the Secretary to ensure our review adequately covered the Departmental level process. In total, we tested 133 reportedly corrected weaknesses of 20 IT systems and 1 program. These systems and program were owned by the Office of the Secretary, the Assistant Secretary of Indian Affairs, the Bureau of Land

Management, the Bureau of Reclamation, the Geological Survey, the Minerals Management Service, and the National Park Service. (See Appendix 3 for the specific systems tested.)

EVALUATION CRITERIA

Public Law 107-347

Federal Information Security Management Act of 2002 (**FISMA**). This Act requires federal executive branch agencies to develop a process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in information security policies, procedures, and practices.

Office of Management and Budget Circular and Memoranda Circular A-130 "Management of Federal Information Management Resources." This Circular among other issues related to IT states that:

- Application of up-to-date information technology presents opportunities to promote fundamental changes in agency structures and work processes that improve the effectiveness and efficiency of federal agencies.
- Planning for information systems should include intended uses of the system, budgeting, and acquisition.
- Government information should be protected commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information.
- Sufficient information should be recorded, preserved, and made accessible to ensure the management and accountability of agency programs.
- Improvements to existing information systems and the development of planned information systems should not unnecessarily duplicate IT capabilities within the same agency, from other agencies, or from the private sector.
- A selected system or process should maximize the usefulness of information and preserves the appropriate integrity, usability, availability, and confidentiality of information throughout the life cycle of the information.
- IT needs should be met through cost effective intraagency and interagency sharing before acquiring new IT resources.
- The agency head should appoint a Chief Information
 Officer who must report directly to the agency head to
 carry out the responsibilities of the agency. The Chief
 Information Officer must be an active participant
 throughout the annual agency budget process in
 establishing investment priorities for agency information
 resources.

The agency head should direct the Chief Information
 Officer to monitor agency compliance with the policies,
 procedures, and guidance in this Circular. The Chief
 Information Officer should develop internal information
 policies and procedures and oversee, evaluate, and
 otherwise periodically review agency information
 resources management activities for conformity with the
 policies set forth in this Circular.

Memorandum M-03-19, "Reporting Instructions for the Federal Information Security Management Act [FISMA] and Updated Guidance on Quarterly IT Security Reporting." This Memorandum describes the requirements for quarterly IT security reporting through OMB's POA&M. This guidance is applicable to POA&M reporting during fiscal year 2004.

Memorandum M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act" (FISMA). This Memorandum describes the requirements for quarterly IT security reporting through OMB's POA&M. This guidance is applicable to POA&M reporting during fiscal year 2005.

Department of the Interior Policy and Guidance

Departmental Manual (375 DM 19) "Information Technology Security Program." This Manual chapter establishes policies, assigns organizational and management roles and responsibilities, and establishes minimum requirements for the development, implementation, maintenance, and oversight of an IT security program for protecting the Department's information and IT systems that store, process, or transmit unclassified information.

IRM [Information Resources Management] Directive 2004-009 "Revised Reporting Instructions for DOI's POA&M." This directive includes the Department's timelines for fiscal year 2004 POA&M reporting. In addition, the directive includes attachments that describe the Department's POA&M process and reporting guidance.

Instructions for POA&M Reporting. The Department provided an Excel spreadsheet with instructions for each data field to the bureaus for POA&M reporting.

Summary Results of Weaknesses Tested from Bureaus' Plans of Actions and Milestones, September 15, 2004 and December 15, 2004

Bureau and System Plans of Action and Milestones	Number of Corrected Weaknesses Reported	Number of Corrected Weaknesses Tested	Number of Corrected Weaknesses Determined Not Corrected
Office of the Secretary Security Program Aircraft Management Local Area Network General Support System (AM LAN) Alaskan Regional Telecommunications Network (ARTNET) Denver Data Center General Support System Enclave (DDCGSS) Interagency Aircraft Services Local Area Network General Support System (IAS LAN) Quarters Management Information System (QMIS) Reston Local Area Network General Support System (Reston LAN) Safety Office Local Area Network (SO-LAN)	104	15	12
Assistant Secretary of Indian Affairs Asset Management System (AMS) Educational Native American Network 2 (ENAN-2) Fee to Trust (FTT)	26	16	8
Bureau of Land Management BLM Enclave General Support System	30	20	5
Bureau of Reclamation Denver Office General Support System (DOGSS) Columbia Basin Supervisory Control and Data Acquisition (CBP SCADA) Hydrological and Meteorological Information System (HMIS) Mid-Pacific Regional General Support System (MPGSS) Safety and Security Information System (SSIS)	48	17	6
Geological Survey National Map	81	40	21
Minerals Management Service Technical Information Management System (TIMS) MMS Network (MMSNet)	23	16	8
National Park Service NPS One General Support System	32	9	4
Total	344	133	64

POA&M PRACTICES AND AUTOMATED SYSTEM CAPABILITIES FROM DEPARTMENT OF THE INTERIOR BUREAUS AND THE ENVIRONMENTAL PROTECTION AGENCY

During our evaluation we identified promising practices that we believe could be used by the Department of the Interior (Department) to improve its plan of action and milestones (POA&M) process. We also identified capabilities from two automated systems that would improve the Department's automated POA&M system.

AREA

Documenting management accepted risks of security weaknesses.

PRACTICE

The Bureau of Reclamation's (BOR) "System Security Risk Acceptance Form" provides a standard template for senior management to document acceptance of low risk weaknesses. Low risk weaknesses are those that do not impact the certification and accreditation that the system adequately safeguards data or that do not adversely impact operations. BOR's guidance, as it relates to the Form, requires that the information technology (IT) system owner, regional IT security manager, and BOR's Chief Information Officer review accepted security weaknesses no less than annually.

The Minerals Management Service includes a cost/benefit analysis as part of its justification for acceptance of risk.

Keeping system owners updated on the status of security weaknesses.

The National Business Center's IT Security Manager sends a monthly POA&M report to system owners. The report shows the status of the corrective actions for IT security weaknesses that are ongoing and on target for completion and of each weakness that is ongoing but not on target for completion.

Using POA&Ms as a management tool at all levels in a bureau.

For one of the Bureau of Land Management's (BLM) IT systems, "working POA&Ms" are maintained for subsets of the system. In this case there is a subset for each of BLM's 13 state offices. Each "working POA&M" has a description of each weakness in that subset's part of the system as well as a description of the respective corrective actions. Each state office uses the "working POA&M" to manage the IT security weaknesses in its state. BLM, because the subset weaknesses have common identifiers, uses the "working POA&Ms" to prepare BLM's quarterly POA&M which is submitted to the Department.

As part of our evaluation, we interviewed personnel from the Assistant Secretary for Indian Affairs and the Environmental Protection Agency who demonstrated effective capabilities in their automated POA&M systems that the Department could use to improve its automated POA&M system.

CAPABILITY

DESCRIPTION

Classify IT systems as either a major application or a general support system.

The POA&M system asks questions that when answered by the user the system helps the user to classify the IT system as either a major application or a general support system. A major application requires a different set of controls than a general support system to safeguard information.

Identify weaknesses and update POA&M.

The POA&M system contains the National Institute of Standards and Technology's Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, self-assessment questionnaire. At the same time as the user completes the questionnaire, the system automatically identifies weaknesses and updates the POA&M.

Track requirements for an IT system to be certified and accredited as adequately protecting data.

The POA&M system tracks whether a system meets the requirements for it to be certified and accredited as adequately safeguarding data. These requirements include: the system must have undergone a risk assessment, the system must have undergone a self-assessment, the system must have a security plan describing all the controls that protect the system, and the system must have a contingency plan to recover in the event of a system failure or disaster.

Associate controls to applications supported by a general support system.

The POA&M system associates the controls in a general support system to the major applications supported by that general support system.

Contains standardized data on security weaknesses.

The POA&M system contains standardized descriptions of weaknesses and related corrective actions. When necessary unique weaknesses can also be added to the system.

Tracks the completion of corrective actions.

The POA&M system tracks the completion of corrective actions for standardized weaknesses. The system ensures that the scheduled corrective actions are in an appropriate order and does not allow weaknesses to be reported as corrected before all information supporting the completion of the corrective actions has been input into the system.

CAPABILITY	DESCRIPTION
Allows queries of weakness data.	The POA&M system allows queries to obtain data regarding IT security weaknesses including the progress of corrective actions. In addition, the system can generate POA&M reports in OMB's required format.
Maintain history of weaknesses.	Maintains records of weaknesses that were corrected and allows corrected weaknesses to be re-opened if necessary.



United States Department of the Interior

OFFICE OF THE SECRETARY Washington, DC 20240



Memorandum

SEP | 4 2005

To: Assistant Inspector General for, Audits

Office of Inspector General,

From; W. Hord Tipton

Chief Information Officer

Subject: Response to "Draft Evaluation Report on the Department of the Interior's

Process to Manage Information Technology Security Weaknesses

(Assignment No. A-EV-MOA-0001-2005)."

Thank you for the opportunity to respond to the "Draft Evaluation Report on the Department of the Interior's Process to Manage Information Technology Security Weaknesses (Assignment No. A-EV-MOA-0001-2005)." The Plan of Action and Milestones (POA&M) process is a vital component of the Department's Information Technology (IT) security program. As you know, Interior made significant progress in establishing and implementing a department-wide POA&M process, to the point where the Office of Inspector General concluded in 2004, "Based on our examination of the Department's instructions for the development and implementation of POA&Ms, we concluded that as designed, the POA&M process is effective and satisfies the pertinent Federal guidance presented in Attachment C of Office of Management and Budget Memorandum 03-09 Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting issued August 6, 2003."

We note that, as our program has matured, OIG evaluations have become more rigorous as well. We appreciate that this increased level of evaluation will allow us to continue to mature and improve our processes, and thus our IT security, beyond minimum requirements. Please note that improvement of IT security beyond documented OMB or NIST requirements may not be our highest priority for available critical IT security funding. However, as we evaluate our overall IT security funding needs and available resources, we will consider recommendations in light of priorities in the program.

We appreciated meeting with OIG staff and management early in this evaluation process. These meetings provided us an opportunity to begin immediate implementation of proposed recommendations. Our immediate action significantly improved our processes during this fiscal year. We also appreciate that BOR, MMS, NBC, and BLM were specifically noted for effective implementation of POA&M practices. These and other practices served as the basis for improved guidance Department-wide.

Our responses to the recommendations are outlined below.

Recommendation 1:

Institute a quality assurance process to ensure:

- All weaknesses are reported.
- b) Weaknesses are completely described and the respective corrective actions would adequately correct the weaknesses. This could be partially addressed through establishing standardized descriptions of common weaknesses and related corrective actions.

Response:

a) Quality assurance programs are an important part of a maturing process. Based on OIG recommendation, the Department issued guidance requiring, "Each IT security weakness identified in any review of a program or system must be entered on the authoritative POA&M (e.g., all Notice of Findings and Recommendations (NFRs) from OIG audits, Security Test and Evaluation (ST&E) and risk assessment reports, NIST SP 800-26 self-assessments, internal/external penetration testing, vulnerability scanning, site/facility compliance reviews, C&A package compliance reviews, etc.)."

OMB guidance may not have kept pace with incident management requirements and vulnerability monitoring tools or capabilities often employed by Federal agencies. Incident management procedures at many Federal agencies require officials to employ immediate action to safeguard systems and data from outside threats or vulnerabilities. The management of such rapidly handled changes may be better addressed through other processes. Furthermore, it may not be prudent to disclose such vulnerability details in POA&Ms. The use of vulnerability monitoring tools should also be considered as an acceptable adjunct to the POA&M. Since these tools often provide misleading results or false-positives and other errors, the information needs to be screened before putting information in POA&Ms and should still be summarized.

b) We initiated a quality assurance process by OCIO Directive 2005-007, May 3, 2005, with which all bureaus complied. Copies of bureau and office verifications have been provided to your office. We used our experience with this initial process and the recommendations provided in your report to refine and clarify our procedures, as issued by memorandum of August 18, 2005. However, we plan to issue additional guidance in a new OCIO Directive and POA&M Process Standard for implementation in FY 2006 to further enhance POA&M processes. This additional guidance has been developed by a team of specialists from throughout the Department and will provide more recommended standardization.

OMB M-04-25 states that "sensitive descriptions of the specific weakness are not necessary" (p. 15) and endorses the use of general or brief descriptions. A template

attached to the OMB memorandum also provided examples on the type of descriptive information required on IT security weaknesses. The example illustrates that high-level descriptions of IT security weaknesses is acceptable. Separate source documents and reports detail more fully each finding described in the POA&M, and provides adequate traceability.

We believe the implementation of the existing quality assurance process fully implements this recommendation.

Recommendation 2:

Institute a verification process to ensure that weaknesses reported as corrected are, in fact, corrected; that supporting documentation is maintained; and that management's acceptance of risk is appropriately justified and documented.

Response:

We initiated a quality assurance and verification process by OCIO Directive 2005-007, May 3, 2005, with which all bureaus complied. Your office has been provided copies of bureau and office verifications that weaknesses that were reported as corrected were in fact corrected. We used our experience with this initial process and the recommendations provided in your report to refine and clarify our procedures, as issued by memorandum of August 18, 2005.

However, we also intend to issue a new OCIO Directive and POA&M Process Standard for implementation in FY 2006 to further enhance the POA&M process. This additional guidance has been developed by a team of specialists from throughout the Department and will provide much of the recommended standardization. The POA&M Process Standard will provide for an additional quality assurance process, to be performed by the OCIO, which will include inspection and review of a sample set of completed POA&M corrective actions each fiscal year.

The use of cost benefit analyses is recommended along with other factors to be considered when making such decisions. However, it is not cost effective for agencies to complete cost-benefit analyses for every security weakness that falls into the risk acceptance category.

We believe the implementation of the existing quality assurance and verification process fully implements this recommendation.

Recommendation 3:

Require senior bureau management to certify that information in the bureaus' POA&M is accurate and true.

Response:

The quality assurance and verification process initiated by OCIO Directive 2005-007, May 3, 2005, and further clarified by memorandum of August 18, 2005, requires senior management officials to ensure and verify information in the bureau's POA&M is accurate.

We believe the implementation of the verification process fully implements this recommendation.

Recommendation 4:

Institute a practice to review all Department IT system and program weaknesses to ensure the most critical weaknesses for the most critical systems of the Department are being addressed first.

Response:

Interior agrees with the spirit of this recommendation, but not the recommended corrective action, for the following reasons:

- The Department receives its IT budget under the authority of multiple appropriations, and with specific restrictions on movement of appropriated funds among bureaus or programs. The recommendation for Department-wide prioritization of POA&M funding does not take into account the statutory restrictions, nor the practical implications of managing these investments. Interior's policy is clear that any risks determined critical or unacceptable <u>must</u> be fully funded for immediate mitigation and <u>all</u> risks above residual must be planned and funded within the Designated Approving Authority's (DAA) budget. Thus, prioritization across bureaus is not a relevant issue.
- NIST SP 800-37 requires the DAA to make the final decision, and be held
 accountable, for accepting risks to their systems. If officials at other levels in the
 Department make changes to the DAA's determination, it would undermine both the
 DAA's authority and accountability. The DAAs and other senior management
 officials rely on a variety of factors in establishing scheduled commitments to correct
 weaknesses.
- 3. Interior's commitment to implement a planned corrective action to resolve known weaknesses as indicated in the "Scheduled Completion Date" column represents senior management's priority in addressing weaknesses. Both IATO status and/or planned dates for implementing corrective actions represent the DAA's degree of tolerance and duration for continued exposure to risks resulting from identified weaknesses.

- 4. Sequential prioritization based on risk level alone does not make sense in an operational and budgetary context where some weaknesses are more easily and quickly corrected than others. Adhering to a strictly sequential work-off plan could leave a larger number of weaknesses unresolved, which could increase the overall risks to individual systems, potentially raising the system risk to unacceptable levels.
- 5. Interior meets the OMB requirements, as risk levels and severity of weaknesses are identified in Risk Assessment reports and other source documentation. As described in DOI IRM Directive 2004-009 Appendix A, each bureau and office is required to establish a priority process for addressing IT system security weaknesses based on the significance of the vulnerability (See page C-4). Each system security weakness is assigned a priority level of High, Medium, or Low. The Department also established a requirement to address all high priority IT security weaknesses within 180-days. The Department's priority setting process, therefore, is adequate and fully complies with OMB guidance.

We believe no further action is needed to implement this recommendation.

Recommendation 5:

Improve the Department's automated POA&M system. To determine the best automated system for the Department, consult with bureaus' IT operational staff, system owners, program managers, and others that are involved with IT security weakness remediation. Also, canvass other Federal agencies that have implemented automated systems to manage POA&Ms.

Response:

Again, Interior agrees with the spirit of the recommendation, as automation improvements drive many enhancements to processes, and should be evaluated for efficacy. However, without such an evaluation, prescriptive improvements are premature. Nonetheless, Interior recognizes the benefits of using POA&M automation tools and plans to evaluate tools for prospective use in Interior, but may not be able to immediately implement the recommendation nor find it cost effective to do so.

As we evaluate possible automated solutions, please be aware that we must consider the following factors:

- The current POA&M reporting format, while not optimal, meets basic program requirements. At this point, investing in a different POA&M tool may not be the highest priority for limited resources.
- The Department has a structured process, with senior management level
 involvement and approval, for determining the need for automated tools and the
 priority for funding and implementing them. Also, as a new automated POA&M
 system was not included in the FY 2007 decisions, such a system could not be

- funded until FY 2008. We are investigating opportunities for workflow improvement within approved IT security operations and maintenance funding.
- Implementation of a single-purpose system for POA&Ms would be contrary to a standards-compliant, service-oriented, component-based architecture. Many of the functional requirements for security POA&Ms - such as forms automation. workflow automation, and document and records management - are common to other Departmental and OCIO processes, and those requirements should be met with common software service components. Likewise, some of the data required for POA&Ms must be shared with other applications, such as DEAR and eCPIC. and should be based upon a common data architecture that minimizes needless inconsistencies and redundancies, rather than potentially aggravating them through implementation of yet another stovepipe system. OCIO will be applying its Methodology for Business Transformation (MBT) to its own processes and the recommendations derived from the MBT should drive the establishment of priorities for sharing of data, retirement and/or consolidation of existing systems, and implementation of new capabilities. Through this process, we are also validating requirements with our bureaus, completing tool assessments and developing an investment proposal to be considered in the next capital planning cycle.

We believe we are compliant with OMB-specified POA&M reporting using the existing spreadsheet format, and therefore meet the requirements of this recommendation.

In summary, we believe we addressed all recommendations, eliminating any need to elevate concerns to the level of a material weakness for this fiscal year. We worked diligently to implement past and current OIG recommendations, and are committed to continued enhancements in our POA&M program. The assistance provided by OIG in identifying opportunities to strengthen the program was very valuable. Our current POA&M program meets OMB and NIST requirements, despite the many challenges in implementation this year, including staff turnover and unprecedented consumption of resources by the Department's largest civil case (Cobell v. Norton). Nonetheless, the Department's program continues to improve in maturity, awareness, accountability, integrity, efficiency, and quality assurance.

Recommendation and Implementation Status

Recommendation	Responsible Individual and Office	Status
1	W. Hord Tipton, Office of the CIO	completed
2	W. Hord Tipton, Office of the CIO	completed
3	W. Hord Tipton, Office of the CIO	completed
4	W. Hord Tipton, Office of the CIO	completed
5	W. Hord Tipton, Office of the CIO	completed

In general, this Evaluation Report is timely and provides constructive feedback for the POA&M program and process. We proactively incorporated the recommendations

presented here, such that they can now be considered fully implemented. I believe the POA&M process, following OMB direction, provides a sound program for managing the remediation of IT security weaknesses. I look forward to a continued positive relationship with your office as we further mature our IT security programs.

If you have any questions, please contact me at 202-208-6194. Staff may contact Mr. Larry Ruffin at 202-208-5419.

Attachments

- OCIO Directive 2005-007, May 3, 2005
- Memorandum of August 18, 2005
- Draft POA&M Guidance

cc: Lynn Scarlett, AS/PMB

Appendix 6

STATUS OF EVALUATION RECOMMENDATIONS

Recommendation	<u>Status</u>	Action Required
1, 2, 3, 4, and 5	Unresolved.	Reconsider the recommendation, and provide a corrective action plan that includes target dates and titles of officials responsible for implementation.

Report Fraud, Waste, Abuse, and Mismanagement

Fraud, waste, and abuse in government concerns everyone: Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or Insular Area programs and operations. You can report allegations to us in several ways.

By Mail: U.S. Department of the Interior

Office of Inspector General Mail Stop 5341 MIB 1849 C Street, NW

1849 C Street, NW Washington, D.C. 20240

By Phone: 24-Hour Toll Free 800-424-5081

Washington Metro Area 202-208-5300

OF INSPECTOR

By Fax: 202-208-6081

ARCH 3, 18

By Internet: www.oig.doi.gov

Annual Evaluation

Information Security Program

Report No. A-EV-MOA-0006-2004

October 2004

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

October 6, 2004

To: Secretary

From: Earl E. Devaney

Subject: Annual Evaluation of the Information Security Program of the Department of

the Interior (Report No. A-EV-MOA-0006-2004)

This report presents the results of our annual evaluation of the information security program of the Department of the Interior (Department). The evaluation is required by the Federal Information Security Management Act of 2002.

We found that the Department continues to improve the security over its information systems. However, despite sound guidance from the Office of the Chief Information Officer, we continue to identify weaknesses in bureau and office implementation of IT security requirements.

If you have any questions about this report, please do not hesitate to call me at (202) 208-5745.

INTRODUCTION

This report presents the results of our evaluation of the information security program of the Department of the Interior (DOI). The objective of our evaluation was to determine whether DOI's information security program satisfied the requirements of the Federal Information Security Management Act of 2002 (FISMA)¹ and to obtain information necessary to respond to questions about DOI's security programs from the Office of Management and Budget.²

The need for information-system interoperability demands effective management, oversight, and coordination of efforts to address security risks. The Congress enacted FISMA to provide a comprehensive framework to secure the federal government's information and information technology (IT) systems. FISMA requires federal agencies to implement security programs that protect information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. Specifically, FISMA requires, overall, that a security program equip federal agencies with mechanisms to do the following:

- ✓ assess risks and implement policies and procedures to reduce risks;
- ✓ test and evaluate security controls;
- ✓ plan for continuity of operations;
- ✓ maintain subordinate plans for providing information security;
- ✓ plan for security throughout life cycle of systems;
- ✓ plan corrective actions;
- ✓ train employees and contractors; and
- ✓ detect, report, and respond to security incidents.

To accomplish our objective we did the following:

- ✓ reviewed and assessed documentation supporting the accomplishment of security program requirements;
- ✓ analyzed recently completed Government Accountability Office (GAO), Office of Inspector General (OIG), and DOI reports related to IT security; and
- ✓ tested controls over 20 of DOI's 157 information systems 9 major applications and 11 general support systems. These tests included the performance of limited non-intrusive scanning of DOI networks and devices, such as servers and firewalls, which were accessible from the Internet.

.

^{1 44} II S C 8 35

² Memorandum M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act, August 23, 2004

We did not cover DOI's national security information systems because they are subject to review by the Central Intelligence Agency. Appendix 1 presents further details on our evaluation methodology.

The results of our evaluation are presented in the body of the report and our responses to OMB questions about DOI's security program are presented in Appendix 2.

RESULTS OF EVALUATION

We found that DOI has effectively designed its information security management program to meet the requirements of FISMA and continued to improve security over its information systems (see Appendix 3 for accomplishments). DOI developed its information security program based on OMB policies, NIST standards and guidelines, and DOI policies established through departmental directives. We also observed that the DOI Chief Information Officer (CIO) developed a separate scorecard and action plan to track bureaus' and offices' (bureaus) progress in meeting FISMA requirements and that the CIO regularly reports to the Secretary and senior management on the status of DOI's information security program. However, despite these efforts, our review of information and actions reported by bureaus indicated that they have not consistently followed DOI guidance in implementing their security programs. In particular, our tests of 20 systems, 19 of which were certified and accredited³ by the bureaus, identified weaknesses in the conduct of a majority of the system certifications and accreditations. In our opinion, this demonstrates a clear need for qualitative examination by the CIO of reported bureau accomplishments.

Our analysis of DOI's overall performance related to key FISMA requirements is presented in the following paragraphs, and Appendix 4 summarizes those FISMA requirements directly related to systems where we identified weaknesses in our review of 20 DOI systems.

ASSESS RISKS

The objective of risk management is to enable an agency to accomplish its mission(s) by (1) better securing the IT systems that store, process, or transmit information; (2) enabling

management to make well-informed risk-management decisions to justify the expenditures that are part of an IT budget; and (3) assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

According to DOI policy, NIST Special Publication 800-26, "Security Self Assessment Guide for Information Technology Systems" (NIST SP 800-26) can be used, in conjunction with a technical vulnerability assessment, to establish an initial risk assessment for each system. DOI policy also requires that a full risk assessment be

³ An information system accreditation, according the National Institute of Standards and Technology (NIST), is the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls. The information needed to support an accreditation is developed during detailed assessments of system risks and tests of controls to determine whether controls are properly implemented. The results of these efforts are then reflected in updated system security plans. In effect, the process to certify and accredit systems incorporates most key requirements of FISMA.

performed on each system prior to granting system certification and accreditation. In order to establish a full risk assessment, DOI's certification and accreditation process states that NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems" (NIST SP 800-30), must be used.

We found that 12 of the 19 certified and accredited systems (63 percent) did not have risk assessments that followed NIST SP 800-30 guidance. For example, the National Business Center did not have a supporting risk assessment for one of its accredited systems, and the risk assessments for six other systems were based on NIST 800-26 evaluations. We also found that the two systems we tested - one at the Office of Surface Mining Reclamation and Enforcement and the other at U.S. Fish and Wildlife Service - did not have full risk assessments to support their accreditations. In addition to the 12 systems that did not meet NIST 800-30 guidance in their assessments, we also found that two systems did not assess the risks at all locations which operated the systems or did not recognize the risks associated with system connections to other systems.

Although bureaus implemented security controls in all systems we reviewed, they lack assurance that controls implemented were the most effective for mitigating any related risk or that the cost of the security control was justified because all risks to systems and information were not identified or evaluated.

TEST SECURITY CONTROLS

DOI policy requires that information system security controls and techniques undergo periodic testing and evaluation. DOI policy also requires that for certification and accreditation, a system must undergo formal security tests and evaluations

(ST&E). DOI completed periodic testing of its security controls through one or more of the following: 1) annual reviews using NIST SP 800-26; 2) ST&E; and 3) external vulnerability scanning of its networks.

We found that bureaus conducted internal evaluations using NIST SP 800-26 guidance on all of the 20 systems in our review. In addition, we determined that 84 percent of the accredited systems we reviewed (16 of 19 systems) underwent testing of controls through an ST&E process. However, we found that at least 3 of the 16 ST&Es did not cover all system components or locations and that 3 systems were certified and accredited without the benefit of an ST&E. As a result, not all controls over information systems had been properly evaluated for their effectiveness.

We also determined that DOI conducted monthly SANS/FBI Top 20⁴ vulnerability scans of its external networks (systems) that can be accessed from the Internet. As a result of the scans, the bureaus reported that their external networks did not have any of the "Top 20" vulnerabilities.

4

⁴ SysAdmin, Audit, Network, Security (SANS) and the FBI [Federal Bureau of Investigation] identified the top 20 vulnerabilities to information system security.

PLAN FOR CONTINUITY OF OPERATIONS

DOI policy requires that for a system to be accredited, contingency plans in accordance with NIST and DOI guidance must be developed and tested. Of the 19 systems certified and accredited, 16 had contingency plans. However, we found deficiencies in 12 of these plans. The following are

examples of these deficiencies:

- Six of the contingency plans had not been tested.⁵
- In four of the tested plans for National Business Center systems, we found that test results were not adequately documented or plans were not updated to reflect the test results.
- For the Bureau of Reclamation's Wyoming Area Office Supervisory Control and Data Acquisition system, the IT contingency plan, which addresses the specifics of restoring the system, was not integrated with the Emergency Action Plan, which covers the physical relocation of personnel and systems in the event that the facility is destroyed.
- For Indian Affairs' TrustNet, the contingency plan was limited to only technical procedures and did not identify a team for the recovery operations or include the specific steps to recover from a disruption in service. Additionally, the plan did not show the order of priority for recovering critical applications.

MAINTAIN SUBORDINATE PLANS FOR INFORMATION SECURITY

DOI policy requires that a system security plan be developed for each system and that the plan be updated every three years or if significant changes are made to the system. The system security plan should provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and establishes rules of behavior concerning the use of the system. DOI recognized that

system security plans needed improvement and required bureaus to perform independent reviews of their respective system security plans. Despite this effort, we identified deficiencies in security plans for 17 of the 19 accredited systems reviewed. Specifically, the plans failed to always do the following:

• identify the specific system security controls to permit effective testing of the controls,

⁵ Bureau of Land Management's Perimeter/DMZ, National Interagency Fire Center Enclave, Wildland Fire Management Information System; Bureau of Reclamation's Denver Office general support system; Indian Affairs' TrustNet; and Office of the Special Trustee for American Indians' OSTNet.

- clearly differentiate between planned and actual controls,
- identify current system contact and management information,
- appropriately assign system security responsibilities,
- include correct interconnection information,
- include the applications supported by general support systems, and
- include updated information based on the tests of controls and identified risks.

Consequently, DOI lacks assurance that it has an adequate overview of each system and the system control environment.

PLAN FOR SECURITY THROUGHOUT SYSTEM LIFE CYCLE

DOI policy requires that funding for IT security be an integral part of each system's life cycle. In our review of 20 systems, we found that security costs were only fully integrated into the life cycle of 12 systems (60 percent). To be most effective, information security funding should be fully integrated into the life cycle of each system. Without integration of IT security requirements and related costs in the development, implementation, maintenance, and disposal phases of an IT

system, bureaus lack assurance that they have the most cost-effective security controls implemented.

PLAN CORRECTIVE ACTIONS

DOI established a Plan of Action and Milestone (POA&M) process consistent with OMB guidance. The guidance requires that POA&Ms (1) include all security weaknesses found during any review done by, for, or on behalf of the organization, (2) represent a prioritization of remediation activities, (3) be tied to the

organization's budget submission through the unique project identifier of a system, and (4) be used as an active project management tool. Based on the 20 systems we reviewed, we found that bureaus recorded known weaknesses in their POA&Ms most of the time (84 percent). However, we also found a need to ensure that all reported weaknesses are recorded, priorities are assigned to correct all weaknesses, and costs needed to remedy weaknesses are always identified. Our review specifically found the following:

 Agreed-upon weaknesses identified in notices of findings and recommendations during OIG audits of bureau financial statements were not always included in the POA&Ms or were not included in the POA&Ms until after the final audit reports were issued.

- Bureaus did not incorporate all weaknesses identified through risk assessments and ST&Es into their POA&Ms for 6 of the 20 systems reviewed.
- Remediation activities were not prioritized in the POA&Ms in three of the systems reviewed.
- Resources were not always allocated based on prioritization of the weakness. For example, in Bureau of Land Management's POA&M for the BLM Enclave, there were 20 weaknesses reported as high priority. The POA&M identified the resources needed to correct only 5 of these high priorities. However, other weaknesses classified as medium in this same system had resources identified. Consequently, it is difficult for the bureau to ensure that highest priority weaknesses will be addressed first.
- Resources required to complete remedial actions were not tied directly to the budget documents 56 percent of the time, based on our review of 10 bureau budgets and POA&Ms. Thus, bureaus do not have full assurance that required resources would be allocated to correct the weaknesses.
- POA&Ms were not always developed for all components of an information system that had weaknesses, such as state, regional, and field offices' local area networks which represent parts of bureaus' general support systems. Therefore, POA&Ms were not used to track remedial actions at these state, regional, and field offices.

TRAIN EMPLOYEES & CONTRACTORS

DOI policy requires all users, including contractors, of IT systems to receive annual security awareness training. The policy also requires training for all levels of personnel involved with IT systems including system managers, system owners, operators, IT security staff, and executives. We found that DOI

provided annual security awareness training to a majority of its personnel and specialized training to managers with significant information security responsibilities. However, DOI had the following deficiencies:

- DOI had no specific methodology to identify all contractors with access to DOI systems. Also, DOI had no documented criteria for excluding employees from the required training and documenting the basis for the exclusions.
- DOI had not identified all of the individuals with significant information security responsibilities. DOI reported that approximately 1,200 individuals had significant security responsibilities. However, we believe that the total may be

⁶ DOI excluded groups of employees such as firefighters, seasonal employees, employees who do not touch a computer system, employees on medical leave, and new employees without access to computer systems.

over 2,000 based on the fact that DOI has more than 76,000 individuals with access to its systems and over 2,000 operating locations.

• DOI had not developed and implemented a program that would ensure those individuals with significant security responsibilities received specialized training that related to the duties performed.

RESPOND TO SECURITY INCIDENTS

FISMA requires that each agency information security program include procedures for detecting, reporting, and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done; notifying and consulting with the Federal information security incident center

(US-CERT) and notifying and consulting with law enforcement agencies and relevant Offices of Inspector General. DOI has issued a handbook for incident response which requires each bureau to develop bureau-specific computer security incident response procedures and describe the specific implementation of the DOI handbook. We found that 7 of the 10 bureaus reviewed had finalized procedures to augment the DOI's Incident Response Handbook. Of the three bureaus that had not finalized incident response procedures, two bureaus were drafting procedures and one bureau opted to use only DOI's handbook.

OTHER MATTERS

In addition to the specific FISMA requirements discussed above, DOI is also focusing on IT security in its critical infrastructure and Indian trust.

We found that DOI had established a process that included a review of all DOI systems to identify national critical infrastructure systems. As part of this process, DOI's Office of the CIO had coordinated closely with the Office of Law Enforcement and Security to address physical security requirements. The process should provide DOI with information to help ensure that its systems are properly classified as national critical infrastructure systems, mission critical systems, or other sensitive but unclassified systems.

DOI information security related to Indian trust data and systems continues to be reviewed and evaluated as a result of the *Cobell v. Norton* case. Because of this court case, parts of DOI, the Indian Affairs and the Office of Special Trustee for American Indians continue to be prohibited from connecting to the Internet. To address the court-related requirements, DOI is re-engineering to standardize and streamline Trust business processes. Also, DOI continues to test its wide-area network against an operational security profile based on SANS/FBI Top 20 vulnerability list. Current tests disclosed that there were no high risk "Top 20" vulnerabilities found for the perimeter telecommunications equipment exposed to the Internet.

RECOMMENDATIONS

We recommend the following:

- 1. The DOI CIO should institute an oversight process to ensure bureaus and offices effectively implement DOI security program requirements. Specifically, the CIO must ensure that:
 - ✓ reported system certifications and accreditations are adequately performed;
 - ✓ budget documentation and POA&Ms can be directly correlated through OMB project/system identifiers to ensure funding addresses security weaknesses;
 - ✓ IT security costs are integrated into each phase of the life cycle of every system;
 - ✓ weaknesses identified during OIG and other internal or external reviews are included in the applicable POA&Ms at the time the weaknesses are identified and agreed to by the bureau;
 - ✓ POA&Ms not only reflect prioritization of weaknesses but also identify the resources necessary to address the higher prioritized weaknesses so that the corrections of high priority weaknesses are performed first;
 - ✓ DOI's specialized training program for certifying and accrediting officials addresses the requirement of (1) security testing and evaluation, (2) developing continuity of operations plans, (3) testing of the continuity plans, and (4) updating continuity plans based on the test results as part of DOI's certification and accreditation process; and
 - ✓ system security plans and contingency plans are developed and updated accordingly to meet DOI and NIST requirements.
- 2. The DOI CIO should consider the following actions to help ensure that DOI's information security program continues to improve:
 - ✓ clarify DOI guidelines to ensure that full risk assessments are performed following NIST SP 800-30, including an analysis of the controls and the risks being mitigated to meet DOI's certification and accreditation process;
 - establish formal criteria for excluding employees from the required annual security awareness training and establish a process for bureaus to document and justify each excluded individual;

- establish criteria to assist bureaus in identifying all positions with significant IT security responsibilities; and
- develop and implement a program to ensure that individuals with significant IT security responsibilities receive specialized training and that the training relates to the duties performed

EVALUATION METHODOLOGY

This evaluation was performed, as applicable, in accordance with Quality Standards for Inspections issued by the President's Council on Integrity and Efficiency. Accordingly, we included such tests of records and other procedures that were considered necessary to accomplish our objectives.

As part of our testing of DOI's information security program we analyzed the following:

- ➤ Office of Inspector General reviews performed during fiscal years 2003 and 2004 and issued during fiscal year 2004 of security practices and general and application controls over information systems supporting park operations and financial operations included in financial statements audits.
- ➤ General Accounting Office and Office of Management and Budget reports issued during fiscal year 2004 that addressed DOI's security practices and controls.
- Status Reports to the Court under the Cobel v. Norton.
- Policies, procedures, and other documentation for 2 additional bureaus (MMS and NPS).
- ➤ Controls over 20 general support systems and major applications used among eight DOI bureaus. We selected these systems based on whether (1) weaknesses were corrected as reported on a system POA&M, (2) a system was reported as certified and accredited, (3) multiple systems or system components were located at a location, or (4) bureau officials requested the system or system component be included in the review. The systems selected were:

Component	System Name	General Support System/ Major Application
Bureau of Land	Perimeter Security/DMZ	General Support System
Management (BLM)	BLM Enclave	General Support System
	National Interagency Fire Center	General Support System
	Enclave	
	Wildland Fire Management	Major Application
	Information System	
Bureau of Reclamation	Denver Office	General Support System
(BOR)	Wyoming Area Office Supervisory	Major Application
	Control and Data Acquisition	
	Central Valley Automated Control	National Critical Infrastructure
	System	Information System, Major

Component	System Name	General Support System/ Major Application
•		Application
Departmental Offices ⁷	Denver Data Center Enclave	General Support System
	Federal Financial System	Major Application
	Federal Personnel and Payroll System	Major Application
	Quarters Management Information System	Major Application
	Interagency Aviation Services Local Area Network	General Support System
	Reston Local Area Network	General Support System
	Interior Department Electronic Acquisition System	Major Application
	Drug Testing System	Major Application
Indian Affairs (IA)	TrustNet	General Support System
Office of Surface Mining Reclamation and Enforcement (OSM)	Western Regional Coordination Center	General Support System
Office of the Special Trustee for American Indians (OST)	OSTNet	General Support System
U.S. Fish and Wildlife Service (FWS)	Service Wide Area Network	General Support System
U.S. Geological Survey (USGS)	Advanced National Seismic System	Major Application

We conducted our tests of controls of systems for fiscal year 2004, as of July 31, 2004, and processes as of September 23, 2004. To conduct our evaluation, we reviewed DOI's certification and accreditation documentation, including asset valuations, privacy impact assessments, risk assessments, self-assessments, security tests and evaluations, risk mitigation plans or residual risk reports, system security plans, continuity of operations plans, tests of continuity of operations plans, certifications, and accreditations. In addition, we tested controls, such as access to systems, access to computer rooms or facilities, back-up and recovery, and system monitoring. We also reviewed position descriptions of various levels of management in DOI, plans of actions and milestones, capital planning documents, the national critical infrastructure determination process, and incident reporting processes. We interviewed DOI and bureaus' management and staff responsible for managing, operating, and maintaining the systems. Additionally, we conducted non-intrusive scans of DOI external networks (those networks and devices that were accessible from the Internet) using Nessus system vulnerability scanning tool.

-

⁷ Departmental Offices includes the Office of the Secretary, which also includes the Office of the Chief Information Officer and the National Business Center; Office of the Solicitor; and the Office of Hearings and Appeals.

In addition, our evaluation included an analysis of the following:

OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF THE INTERIOR

- ➤ Independent Auditors' Report on the Tribal and Other Trust Funds and Individual Indian Monies Trust Funds Financial Statements for Fiscal Years 2003 and 2002 Managed by the Office of the Special Trustee for American Indians (December 2003)
- ➤ Independent Auditors' Report on the Office of Surface Mining Reclamation and Enforcement's Financial Statements for the fiscal Years 2003 and 2002Annual Report of the Office of Surface and Mining (December 2003)
- ➤ Independent Auditors' Report on the U.S. Department of Interior's Consolidated Financial Statements for Fiscal Year 2003 and 2002 (November 2003)
- ➤ Independent Auditors' Report on the National Park Service Financial Statements for Fiscal Year 2003 and 2002 (December 2003)
- ➤ Independent Auditors' Report on the Minerals Management Service's Financial Statements for Fiscal Years 2003 and 2002 (December 2003)
- ➤ Independent Auditors' Report on the U.S. Geological Survey's Balance Sheet for Fiscal Year 2003 (November 2003)
- ➤ Independent Auditors' Report on the U.S. Fish and Wildlife Service's Financial Statements for the Fiscal Years 2003 and 2002 (November 2003)
- ➤ Independent Auditors' Report on the Bureau of Reclamation's Financial Statements for the Fiscal Years 2003 and 2002 (November 2003)
- ➤ Independent Auditors' Report on the Bureau of Land Management's Financial Statements for the Fiscal Years 2003 and 2002 (December 2003)
- ➤ Improvements Needed in Managing Information Technology System Security, National Park Service (March 2004)
- ➤ Draft Independent Auditors' Report on Bureau of Indian Affairs Financial Statements for the Fiscal Years 2003 and 2002 (January 2004)
- ➤ Information Systems Security over Systems and Applications Used by the National Business Center to Provide Services to Non-Department of Interior Clients (August 2004)
- ➤ Management Issues Identified During the Audit of the U.S. Geological Survey's Fiscal Year 2003 Balance Sheet (January 2004)
- ➤ Management Issues Identified During the Audit of the Bureau of Land Management's Fiscal Year 2003 Financial Statements (December 2003)
- ➤ Management Issues Identified During the Audit of the Bureau of Reclamation's fiscal Year 2003 Financial Statements (December 2003)
- ➤ Management Issues Identified During the Audit of the U.S. Fish and Wildlife Service's Fiscal Year 2003 Financial Statements (December 2003)
- ➤ Management Issues Identified During the Audit of the Minerals Management Service's Fiscal Year 2003 Financial Statements (January 2004)
- ➤ Management Issues Identified During the Audit of the National Park Service Fiscal Year 2003 Financial Statements (January 2004)

➤ Management Issues Identified During the Audit of the Office of Surface Mining Reclamation and Enforcements for Fiscal Year 2003 Financial Statements (December 2003)

GOVERNMENT ACCOUNTABILITY OFFICE

- ➤ Report: Information Technology: Departmental Leadership Crucial to Success of Investment Reforms at Interior (September 2003)
- ➤ Report: Project SAFECOM Key Cross-Agency Emergency Communications Effort Requires Stronger Collaboration (April 2004)
- Report: Electronic Government-Potential Exists for Enhancing Collaboration on four Initiatives (October 2003)
- ➤ Report: Information Technology Management: Governmentwide Strategic Planning, Performance Measurement, and Investment Management Can Be Further Improved (January 2004)
- ➤ Testimony: Critical Infrastructure Protection: Challenges in Securing Control Systems (October 2003)
- ➤ Report: Information Security: Status of Federal Public Key Infrastructure Activities at Major Federal Departments and Agencies (December 2003)
- ➤ Report: GEOSPATIAL INFORMATION Technologies Hold Promise for Wildland Fire Management (September 2003)
- ➤ Report: Federal Chief Information Officers-Responsibilities, Reporting, Relationships, Tenure and Challenges (July 2004)
- ➤ Testimony: Information and Technology Management-Responsibilities, Reporting, Relationships, Tenure and Challenges of Agency Chief Information Management (July 2004)
- ➤ Report: Information Security-Agencies Need to Implement Consistent Processes in Authorizing Systems for Operation (June 2004)
- ➤ Report: Plan Needed to Sustain Progress in Establishing IT Investment Management (September 2003)

OFFICE OF MANAGEMENT AND BUDGET

➤ Fiscal Year 2003 Report to Congress on Implementation of E-Government Act (March 2004)

DEPARTMENT OF THE INTERIOR

- ➤ DOI Fiscal Year 2003 Annual Report on Performance and Accountability (November 2003)
- ➤ Status Report to the Court Number 15, For the Period of July 1, 2003 September 30, 2003 (November 2003)
- ➤ Status Report to the Court Number 16, for the Period October 1, 2003-December 31, 2003 (February 2004)

- > Status Report to the Court Number 17, for the Period January 1, 2004-March 31, 2004 (May 2004)
- ➤ Status Report to the Court Number 18, For the Period of April 1, 2004-June 30, 2004 (August 2004)
- ➤ DOI Quarterly Plans of Actions and Milestones submitted to the Office of Management and Budget for the Quarters Ending December 2003, March 2004 and June 2004
- > DOI monthly system inventory and status of certification and accreditation

2004 FISMA Report

Agency:	Department of the Interior	П
Date Submitted:	10/6/2004	
Submitted By:	OIG	
Contact Information:		
Name:	Roger La Rouche	
E-mail:	roger larouche@oig.doi.gov	
Phone:	202-219-0726	

To enter data in allowed fields, use password: fisma

contingency plans have been Percent of Total #DIV/OR #REF! #DIV/DI #DIVIOR #DIVID! #DIV/OR #DV/Q# 10 abivog Number of systems for tested A.2.e. which A.1. By bureau (or major agency operating component), identify the total number of programs and systems in the agency and the total number of contractor operations or facilities. The agency CIOs and IG's shall each identify the total number that they reviewed as part of this evaluation in FYO4, NIST 800-26, is to be used as guidance for these reviews. Total A.2. For each part of this question, identify actual performance in FYD4 for the total number of systems by bureau (or major agency operating component) in the format provided below Percent of Total contingency plan #DIVIDE #DIVIDE #DIVID# BUNDA systems with a 名の日 #DIVID# Number of A.2.d. 16 Total Percent of Total security controls have been tested and evaluated in systems for which #CIVIDI #CIVIDI #CINOD! #CIVID# **MOINNO!** #CIVOD! #DIVIDE #DIVID# #DIVID# #CIVID# the last year Number of A.2.a. 20 Total Percent of Total IOWIG# costs integrated into the life cycle #DIVIOR #DIVIOR #DIVIOR #DIVIO #DIVIOR MDIVIOR #DIVIOR #DIVIO! #DIVIOR #DIVIOR #DIVID# security control HDIVIOR Number of systems with of the system 12 Total Percent of Total 19 #DIVIOR systems certified #DIVIO! #DIVIOR #REF! #DIVIDI #DIVIOR #DIVIOR IOVAIGE #DIVID! #DIVIO! #DIVIOR HOWICE HOMICH #DIVIOR #DIVIOR #DIVID! #DIVID! #DIVIOR and accredited Number of Number FY04 Contractor Operations or Section A: System inventory and IT Security Performance NOTE: ALL of Section A should be completed by BOTH the Agency CIO and the OIG. Total Number FY04 Systems A.1.b. Total To enter data in allowed fields, use password: fisma Number Reviewed FY04 Programs A.1.a. Total of Surface Mining Reciamation Office of the Secretary andudes NBC. Systems Covered by Other OKS Revisees: Office of the Special Trustee for American Indiana U.S. Fan and Waldlik Service Minerals Management Service Bureau Name U.S. Cardograf Survey Natural Park Service Indian Affairs Subtotols

Comments: Our responses to question A.1.b included those systems evaluated specifically as part of FISMA (20), included in other OKS reviews of IT areas (2), and included in our financial statement audits (52). Our responses to A.2.a are based on the subset of 20 systems evaluated specifically as part of FISMA. The systems covered by other OKS reviews addressed objectives not specifically related to the OMB questions.

_

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

Bratement Brassancy CIO have used appropriate methods to ensure that contractor provided services or pency that the spanning of the spanning of the spanning security policy, and against policy. Spanning and verification of the against systems, and contractor operations of facilities. Admost Always, or development and verification of the against systems, and contractor operations of facilities. Admost Always, or development and verification of the against systems, and contractor operations of facilities. Admost Always, or development and verification of the against a forestations of bureaus (or major operations of programs, systems, and contractor operations of bureaus (or major operations). Statement Statement Nosaly, or 61 Nosaly, or 61 Nesses systems for a-authoritication risk.	A.3. Evaluate the degree to which the following statements reflect the status in your agency, by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Comment area provided below.	in the drop down menu. If appropriate or necessary, include
gency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or inches provided by another agency to their program and systems are adequately secure and meet the requirements of MA. CMB policy and NIST guidelines, national security policy, and agency policy. The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST self-assessment guide. The agency maintains an invertiory of major IT systems and this inventory is updated at least annually. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities. Statement The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) in the agency. Statement	Statement	Evaluation
The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST ressessment guide. 800-28. In instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used breased all elements of the NIST guide. The agency maintains an inventory of major IT systems and this inventory is updated at least annually. The olig was included in the development and verification of the agency's IT system inventory. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) in the agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components). Statement The agency has begun to assess systems for e-authentication risk.	 Agency program officials and the agency CIO have used appropriate methods to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, CMB policy and NIST guidelines, national security policy, and agency policy. 	Rarely, or 0-50% of the time
In instances where the NIST seal-assessment guide was not used to conduct reviews, the alternative methodology used breased all elements of the NIST guide. The agency maintains an invertory of major IT systems and this inventory is updated at least annually. The OIG was included in the development and verification of the agency's IT system inventory. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) in the agency. Statement The agency has begun to assess systems for e-authentication risk.	 The reviews of programs, systems, and contractor operations or facilities, identified above, were conducted using the NIST seek-assessment guide. 800-28. 	Almost Always, or 96-100% of the time
The agency maintains an invertory of major IT systems and this inventory is updated at least annually. The OIG was included in the development and verification of the agency's IT system inventory. The agency CIO systems and concurs with the major IT investment decisions of bureaus (or major operating components) in the agency. Statement The agency has begun to assess systems for e-authentication risk.	 in instances where the NIST self-assessment guide was not used to conduct reviews, the alternative methodology used addressed all elements of the NIST guide. 	
The OIG was included in the development and verification of the agency's IT system inventory. The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities. The agency CIO reviews and condurs with the major IT investment decisions of bureaus (or major operating components) in the agency. Statement The agency has begun to assess systems for e-authentication risk.	 The agency maintains an inventory of major IT systems and this inventory is updated at least annually. 	Almost Always, or 98-100% of the time
The OIG and the CIO agree on the total number of programs, systems, and contractor operations or facilities. The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) in the agency. Statement The agency has begun to assess systems for e-authentication risk.	 The OIG was included in the development and verification of the agency's IT system inventory. 	Frequently, or 71-80% of the time
The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) in the agency. Statement The agency has begun to assess systems for e-authentication risk.		Mostly, or 81-95% of the time
Statement The agency has begun to assess systems for e-authentication risk.	 The agency CIO reviews and concurs with the major IT investment decisions of bureaus (or major operating components) within the agency. 	Mostly, or 81-95% of the time
The agency has begun to assess systems for e-authentication risk.	Statement	Yes or No
contact anamon information contribute that search alternative that ATO	h. The agency has begun to assess systems for e-authentication risk.	Yes
SELECT STREET, SECURITY	 The agency has appointed a senior agency information security officer that reports directly to the CIO. 	Yes

Comments: A.3.a. Of the contractor services we reviewed, DOI's oversight was generally not sufficient to ensure that DOI information was adequately protected. In August 2004, DOI issued guidance for requirements to be included in IT service contracts. We will evaluate this practice in next year's FISMA review,

A.3.c. We did not respond to this question because the DOI used NIST 800-26 in the 20 systems that we reviewed

A.3.e. We were included in the development of the inventory of systems process. We verified that of the 20 systems tested, each of the 20 systems were included in the DOI inventory, however components of the 20 systems were not always included.

A.3.f. Generally, we agree with the DOI CIO on the numbers of programs and systems; however, we have some disagreements over what constitutes contractor operations and facilities.

A.3.g. We found that the DOLORO reviews major IT investments for those systems that are cross-cutting agency-wide systems, sensitive systems, and those that exceed \$35 million. The approval of business cases for these systems is made by committees, of which the DOLORO is a member. The DOLORO transmits the DOLI mestment portfolio to OMB, however, because of the immaturity of the bureaus' capital investment planning and control process, the DOLORO may not be afforded the opportunity to review and concur with all major bureau-level IT investments.

Section B: Identification of Significant Deficiencies NOTE: ALL of Section B should be completed by BOTH the Agency CiO and the OlG. To enter data in allowed fields, use password: fisma B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practand identify which are repeated from FY03. In addition, for each significant deficiency, in	reficiencies ploted by BC word: fisma cant deficiencies 03. In addition	TH the Agenc cles in policies, on, for each sign	ction B: Identification of Significant Deficiencies TE: ALL of Section B should be completed by BOTH the Agency ClO and the OlG, enter data in allowed fields, use password: fisma B.1. By bureau, identify all FY 04 significant deficiencies in policies, procedures, or practices required to be reported under existing law. Describe each on a separate row and identify which are repeated from FY03. In addition, for each significant deficiency, indicate whether a POASM has been developed. Insert rows as needed.	a separate row
		ı	8.1,	
Bureau Name	Total	Total Number Repeated from FY03	FY04 Significant Deficiencies Identify and Describe Each Significant Deficiency	POA&M developed? Yes or No
Dapartranthistie	n	Ŧ	The Department does not fully comply with Federal francial management systems requirements specified in CME Circular A-130, "Nanegement of Federal Internation Resources."	Yes
Agency Total	1			

Comment. We did not include weaknesses indentified in the POA&Ms because we did not evaluate the significance of reported weaknesses.

19

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

P 0

. K.	ocu, impenienteu, anu si managing an agency-wide pa he following statements reflect the status in your agenc mments in the Comment area provided below.	Evaluation	Mostry, or 81-95% of the time	Almost Always, or 96-100% of the time	Almost Always, or 96-100% of the time	Almost Always, or 96-100% of the time	Almost Always, or 96-100% of the time	Sometimes, or 51-70% of the time	Rarely, or 0-50% of the time	Almost Always, or 96-100% of the time	Frequently, or 71-80% of the time	Sometimes, or 51-70% of the time
Section C: OIG Assessment of the POA&M Process NOTE: Section C should "ONLY" be completed by the OIG. The CIO should leave this section blank. To enter data in allowed fields, use password: fisma	C. Intrody this question, and in the sorting provided below, assess whether the agency has developed, impentation, and is managing an agency-more part action and milestone (POA&A) process. This question is for IGs only. Evaluate the degree to which the following statements reflect the status in your agency choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the Commentaries provided below.	Statement	a, Known IT security weaknesses, from all components, are incorporated into the POASM.	 Program officials develop, implement, and manage POA&Ms for systems they own and operate (systems that support their program or programs) that have an IT security weakness. 	 Program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress. 	d. CIO develops, implements, and manages POASMs for every system they own and operate (a system that supports their program or programs) that has an IT security weakness.	e. CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	 The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses. 	 System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11). 	h. OlG has access to POA&Ms as requested.	 OlG findings are incorporated into the POA&M process. 	 POA&M process prioritizes IT security weaknesses to help ensure that significant IT security weaknesses are addressed in a timely manner and receive appropriate resources.

Comments: C.1.f We believe the DOI CIO uses the POA&M as the authoritative management tool to identify and monitor actions for correcting IT security weaknesses. The OIG uses the POA&M as a management tool in conjunction with the OIG audit tracking system and the Department's Audit and Management Follow-up process for tracking the resolution and implementation of recommendations related to IT identified through OIG evaluations and audits

C.1.g The unique information system identifier on the POA&Ms, in most cases, did not match the unique identifier on the budget documents as required by OMB; therefore, there is little assurance that the POA&M costs were directly tied to the budget requests. Additionally, we found that the costs for security identified in the budget justification documents were sometimes less than the resources identified in the POA&Ms to correct the information system security weaknesses.

order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the Agency's certification and Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be risk assessments and security plans. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated Section C should only be completed by the OIG. OMB is requesting IGs to assess the agency's certification and accreditation process in before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "Standards for Security Categorization of Federal C.1 OIG Assessment of the Certification and Accreditation Process before it became final.

Statement	Evaluation
Assess the overall quality of the Agency's certification and accreditation process.	Satisfactory
Comments: DOI has established an adequate certification and accreditation process. However, based on our evaluation of the 19 accredited systems, not all bureaus have fully implemented DOI's process. For example, 12 of the 19 systems did not have risk assessments that fully met NIST SP 800-30 guidance, only 16 of the 19 systems had contingency plans, and only 10 of these plans had been tested. DOI tracked the accomplishment of required elements for certification and accreditation of systems, but had not evaluated the quality of reported accomplishments. DOI recognized that there are issues in this area and, as a result, recently initiated a quality assurance process that entails the detailed evaluation by independent contractors of certification and accreditation documents submitted by bureaus to ensure all DOI requirements are met. Our rating of satisfactory in this area, in part, is based on the implementation of the new initiative by DOI, the effectiveness of which has not yet been evaluated.	

21

D.1. First, answer D.1. If the answer is yes, then proceed. If no, then skip to Section E. For D.1.a-f, identify whether agencywide security configuration requirements address each listed application or operating system (Yes, No, or Not Applicable), and then evaluate the degree to which these configurations are implemented on applicable systems. For example: If your agency has a total of 200 systems, and 100 of those systems are running Windows 2000, the universe for evaluation of degree would be 100 systems. If 61 of those 100 systems follow configuration requirement policies, and the configuration Almost Always, or 96-100% of the time controls are implemented, the answer would reflect "yes," and "51-70%". If appropriate or recessary, include comments in the Comment area provided Evaluation D.2. Answer Yes or No, and then evaluate the degree to which the configuration requirements address the patching of security vulnerabilities. If appropriate or necessary, include comments in the Comment area provided below. Yes, No. or N/A 765 Yes Yes 18 20 No 20 No 20 ž No £ Other. Specify: Wheless Ethernel, Novell, Firewall, Internet Information Services (IIS), Web Server, Unix and Network Infrastructure. 1. Has the CIO implemented agencywide policies that require detailed specific security configurations and what is the D.2. Do the configuration requirements implemented above in D.1.a-f., address patching of security NOTE: ALL of Section D should be completed by BOTH the Agency GIO and the OIG. To enter data in allowed fields, use password: fisma D.1. & D.2. agree by which the configurations are implemented? c. Windows 2000 Professional a. Windows XP Professional e. Windows 2000 Server f. Windows 2003 Server J. Cisco Router IOS d. Windows 2000 b. Windows NT g. Solaris h. HP-UX k. Oracle Linux vulnerabilities? Convenents: We did not evaluate the implementation of the standards as part of our review of systems as the standards were either not available when systems reviewed.

Section E: Incident Detection and Handling NOTE: ALL of Section E should be complete To enter data in allowed fields, use passwor	Section E: Incident Detection and Handling Procedures NOTE: ALL of Section E should be completed by BOTH the Agency CIO and the OIG. To enter data in allowed fields, use password: fisma	
E.1. Evaluate the degree to below.	E.1. Evaluate the degree to which the following statements reflect the status at your agency. If appropriate or necessary, include comments in the Comment area provided below.	ude comments in the Comment area provided
	E.1	
	Statement	Evaluation
a. The agency	 The agency follows documented policies and procedures for reporting incidents internally. 	Frequently, or 71-80% of the time
b. The agency authorities.	 b. The agency follows documented policies and procedures for external reporting to law enforcement authorities. 	Almost Always, or 96-100% of the time
c. The agency Team (US-CEF	c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT), http://www.us-cert.gov.	Almost Alvays, or 96-100% of the time
	E.2.	
E.2, Incident Detection Capabilities.	blithes.	
		Number of Percentage of Systems Total Systems
a. Hor	 How many systems underwent vulnerability scans and penetration tests in FY04? 	19 0.95
d S	 Specifically, what tools, techniques, technologies, etc., does the agency use to mitgate IT security risk? 	LHS.
	Answer.	
	Routers, Firewalls, IDS, logging, shutting off unnecessary services, antivirus updates, on-line real time monitoring for intrusions, automatic updating of operating systems, backup, change management, authentication, encryption, VPN, etc.	e real time monitoring for intrusions, automatic PN, etc.
Comments		

23

which a patch was vulnerabilities for occurred for available? Number of systems affected, by category, on: successful Number of How many incidents Systems Affected number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category VIII, known F.1. For each category of incident listed: identify the total number of successful incidents in FYD4, the number of incidents reported to US-CERT, and the F.2. Identify the number of systems affected by each category of incident in FY04. If appropriate or necessary, include comments in the Comment area up-to-date C&A complete and Systems Systems Affected F.2.b. up-to-date C&A Systems with complete and Number of Systems Affected F.2.a. enforcement Reported to Number of Incidents Jav. Number of Incidents, by category: "Other". If appropriate or necessary, include comments in the Comment area provided below 1,935,030 400,544 2,335,638 F.1.b. Reported to US-CERT Number of Incidents NOTE: ALL of Section F should be completed by BOTH the Agency ClO and the OlG. F1. F2 & F3 1,935,030 400.544 Number of Incidents F.1.s Reported internally Totals: To enter data in allowed fields, use password: fisma Section F: Incident Reporting and Analysis VI. Sucessful Virus/worm Introduction V. Detection of Malicious Logic III. Denial of Service Attack IV. Website Defacement Root Compromise User Compromise provided below. VII. Other

Comments:

- F.1.a. The figures were provided by the DOI CIO.
- F.1.b. The figures were derived from the DOI CIRC database that automatically reports to US CERT.
- F.1.o. This information is not tracked in DOI.
- F.2. This information is not tracked by DOI or U.S. CERT, therefore no information is available. The information in the above schedule was not verified by OIG.

	ppropriate	responsibilities? If appropriate or necessary, include comments in the Comment area provided below.	responsibilities? If appropriate or necessary, include comments in the Comment area provided below.	ints in the Com	G.1.	ded below.	
G.1.a.	G.1.b.		G.1.c.	ð	G.1.d.	G.1,e.	G.1.L
Total number of Employees that received IT employees in security awareness training FY04 as described in NIST Special Publication B00-50	Employees that received IT security awareness training in FYO4, as described in NIST Special Publication 800-50	ceived IT is training cribed in blication	Total number of employees with significant IT security responsibilities	Employees w security respo received s training, as- NIST Special 800-50 a	Security responsibilities that received specialized training, as described in NIST Special Publications 800-50 and 800-16	Briefly describe training provided	Total costs for providing IT security training in FY04 (in \$'s)
Number		Percentage		Number	Percentage		
81,943 76,888	1	0.938310777			#DIV/OI	C&A, CIRC, CISSP, Annual End User Awareness, SANS, MCSE, Cisco, A+, Oracle.	\$1,799,732
			•	9	G.2.		
				. Yes	Yes or No		
 Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training or any other agency wide training? 	explain poli rity awaren vide trainin	cies regard less training g?	regarding peer-to-peer training, ethics training,	2	No		

25

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

DEPARTMENT OF THE INTERIOR'S IMPROVEMENTS IN SECURITY MANAGEMENT PRACTICES FISCAL YEAR 2004

In fiscal year 2004, the Department of the Interior (DOI) accomplished the following:

- Required bureaus and offices (bureaus) to record all systems (major and minor) in the Department Enterprise Architecture Repository System and stabilized the inventory of general support systems and major applications.
- Required all general support systems and major applications to undergo a review of controls in accordance with the National Institute of Standards and Technology (NIST) Special Publication 800-26.
- Established a process for the certification and accreditation (C&A) of DOI's systems that generally met Office of Management and Budget (OMB) and NIST requirements and provided applicable training on this process.
- Monitored the status of bureau and office completion of system C&As and recently instituted a process to assess the quality of C&As to ensure that OMB, NIST, and Departmental guidance is met.
- Reported 83 percent of DOI information systems obtained C&As.
- Established a process for developing DOI's Plan of Actions and Milestones for reporting and correcting information security weaknesses consistent with OMB guidance
- Established the DOI Computer Incident Response Center for bureaus to report information security incidents and for reporting DOI incidents to United States Computer Emergency Readiness Team (US-CERT).
- Established minimum security configuration standards for some existing technologies such as Unix and various Microsoft Windows operating systems.
- Provided training on information security awareness to DOI employees and contractors.
- Improved integration of DOI's Command Center with managing patches for operating systems.

FEDERAL INFORMATION SECURITY MANAGEMENT ACT REQUIREMENTS WHICH PERTAIN TO SYSTEMS WHERE WE IDENTIFIED WEAKNESSES IN COMPLIANCE

Component	System Name	Assessing Risk	System Testing & Evaluation	Continuity of Operations and testing of the plans	Subordinate Plans for Providing Information Security	Security planning integrated into the systems life cycle
BLM	Perimeter			X	X	X
	Security/DMZ BLM Enclave	X	X	X	X	X
	NIFC Enclave			X	X	X
	WildFire Management Information System			X	X	X
BOR	Denver Office GSS	X		X	X	
	Wyoming Area Office SCADA			X	X	X
Departmental Offices	CVACS Denver Data Center Enclave FFS	X		X	X	
		X		X	X	
	FPPS	X		X	X	
	Quarters Management Information System	X		X	X	
	Interagency Aviation Services LAN	X		X	X	
	Reston Local Area Network	X	X		X	
	IDEAS	X				
	Drug Testing	Not certified	l and accredited	1		
IA	TrustNet	X	X	X	X	

FEDERAL INFORMATION SECURITY MANAGEMENT ACT REQUIREMENTS WHICH PERTAIN TO SYSTEMS WHERE WE IDENTIFIED WEAKNESSES IN COMPLIANCE

Component	System Name	Assessing Risk	System Testing & Evaluation	Continuity of Operations and testing of the plans	Subordinate Plans for Providing Information Security	Security planning integrated into the systems life cycle
OSMRE	WRCC	X	X	X	X	X
OST	OSTNet	X	X	X	X	
FWS	SWAN	X	X		X	
USGS	ANSS	X		X	X	X

X signifies that we identified issues related to the FISMA requirements. The issues vary in significance. That is, an issue could be as simple as not updating a system security plan with the name of the individual assigned responsibility for security to not performing a risk assessment.



U.S. Department of the Interior Office of Inspector General

Audit Report

IMPROVEMENTS NEEDED IN SECURITY MANAGEMENT OF INFORMATION TECHNOLOGY SYSTEMS SUPPORTING ENERGY AND WATER OPERATIONS

BUREAU OF RECLAMATION



Picture courtesy of Bureau of Reclamation

Report No. 2002-I-0004 November 2001

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

NOTICE

This document is a final report of the Office of Inspector General. It is being made available to officials having responsibilities concerning the subjects discussed for their information or review and action.

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

Any questions regarding the use of this final audit report should be directed to the General Counsel's Office, Office of Inspector General, at (202) 208-4356.

EXECUTIVE SUMMARY

IMPROVEMENTS NEEDED IN SECURITY MANAGEMENT OF INFORMATION TECHNOLOGY SYSTEMS SUPPORTING ENERGY AND WATER OPERATIONS BUREAU OF RECLAMATION REPORT NO. 2002-I-0004

BACKGROUND AND OBJECTIVE

The Bureau of Reclamation (BOR) is the Nation's second largest producer of hydroelectric power, generating more than 40 billionkilowatt hours of energy each year from 58 power plants. The BOR is the primary supplier and manager of water in the 17 western states. As the supplier, the BOR delivers water to 1 of every 5 western farmers who irrigate about 10 million acres and provides more than 31 million people with water for municipal, rural, and industrial uses. The BOR uses Supervisory Control and Data Acquisition (SCADA) systems to control and manage hydroelectric energy production and water delivery. The Department of the Interior has identified three of the BOR SCADA systems as national critical infrastructure systems, meaning that the failure of any one of the systems would negatively impact the Nation. These SCADA systems support the Hoover Dam, the Shasta Dam, and the Grand Coulee Dam energy and water operations.

The objective of this audit was to determine the effectiveness of the BOR's general controls over its water and energy critical infrastructure information technology (IT) systems and related systems.

RESULTS IN BRIEF

The BOR's IT security policies, procedures, and practices were not effective in establishing the controls necessary for an effective IT security management program to safeguard critical and related IT systems supporting BOR's energy and water operations. While the BOR has taken actions to address some of its IT security risks, further improvements are needed. The BOR needs to develop and implement security plans for each critical SCADA and related system; authorize IT systems to process; explicitly assign IT security responsibilities for each IT system; establish adequate policies and procedures for firewalls and IT incident handling; designate position sensitivity based on risks associated with duties performed; and establish an adequate IT security training program, security management structure, physical access controls, and IT systems contingency planning.

Although the Department of the Interior designated the SCADA systems that support the Hoover Dam, the Shasta Dam, and the Grand Coulee Dam energy and water operations as national critical infrastructure systems, the BOR disagreed with the designations. According to the BOR, proper asset valuations were not performed to determine whether these systems were national critical systems. The BOR agreed to perform the asset valuations to determine whether these systems should be designated as national critical infrastructure systems.

RECOMMENDATIONS

We made 18 recommendations to improve the BOR's IT security management program. Further, we made one recommendation that the BOR ensure asset valuations of the SCADA systems supporting the Hoover Dam, the Shasta Dam, and the Grand Coulee Dam energy and water operations be performed no later than September 30, 2002 to determine whether these systems should be designated as national critical infrastructure systems.

AGENCY RESPONSE AND OFFICE OF INSPECTOR GENERAL REPLY

In his September 28, 2001 response to the draft report the BOR Commissioner concurred with the 19 recommendations. The Commissioner stated that the BOR has increased the priority of its IT security management program and established specific priorities to improve the BOR IT security program which included the development of specific standards and directives related to IT security. Accordingly, the Commissioner's response is sufficient to consider 9 recommendations resolved and implemented and 10 recommendations resolved but not implemented. The 10 recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

No. 2002-I-0004 ii

A-IN-BOR-001-01-M



United States Department of the Interior

Office of Inspector General National Information Systems Office 134 Union Boulevard, Suite 510 Lakewood, Colorado 80228

November 16, 2001

To:

Commissioner, Bureau of Reclamation

From:

Diann Sandy

Director, National Information Systems Office

Subject: Improvements Needed in Security Management of Information Technology

Systems Supporting Energy and Water Operations, Bureau of Reclamation

(Report No. 2002-I-0004)

The Bureau of Reclamation (BOR) is the Nation's second largest producer of hydroelectric power, generating more than 40 billion-kilowatt hours of energy each year from 58 power plants. In addition, the BOR is the primary supplier and manager of water in the 17 Western States and delivers water to 1 of every 5 western farmers who irrigate about 10 million acres of land. The BOR provides more than 31 million people with water for municipal, rural, and industrial uses. To efficiently control and manage infrastructure needed for the production of electrical energy and delivery of water, the BOR uses automated information technology (IT) systems, known as Supervisory Control and Data Acquisition (SCADA) systems. These SCADA systems are computer-based monitoring and control systems that centrally collect, display, and store information from subsystems in facilities, such as dams, power plants, canals, pumping plants, and other power and water management structures. The SCADA systems support the humansupervised remote control of equipment, devices, and automated functions necessary to safely and efficiently operate the facilities. The Department of the Interior has identified three BOR SCADA systems as national critical infrastructure systems¹. These SCADA systems support the Hoover Dam, the Shasta Dam, and the Grand Coulee Dam energy and water operations. Federal regulations and policies require that all IT systems be safeguarded. (See Appendix 1 for summary of applicable criteria.)

RESULTS OF AUDIT

The BOR has recently performed risk assessments of its IT systems, including SCADA systems; has taken actions, such as developing IT security policies and procedures, installing IT security tools, and requesting funding for its IT security management program, to address these risks; and has recently increased the priority of its IT security management program. Overall, however, the BOR did not have an effective IT security management program. In addition, until recently, the BOR had

¹ The Department of the Interior reported to the National Critical Infrastructure Assurance Office three national critical infrastructure information technology systems under Presidential Decision Directive 63.

not considered the SCADA systems to be included within the definition of IT systems and therefore did not apply IT security standards to these systems.

Without a well-designed IT security management program, IT security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources. Additionally, we believe that the BOR should report to the Department the inadequate IT security management program as a deficiency in complying with regulations

IMPROVEMENTS NEEDED IN IT SECURITY MANAGEMENT

The BOR's IT security policies, procedures, and practices were not effective in establishing the controls necessary for an effective IT security management program to safeguard IT systems supporting energy and water operations. Specifically, the BOR did not have:

- An IT system security plan for each IT system.
- An accreditation (authorized by senior management) for each IT system to process.
- IT security responsibilities explicitly assigned for each IT system.
- Policies and procedures issued prior to implementing IT firewall² security tools.
- Adequate policies and procedures for IT incident handling.
- Position sensitivity based on risks associated with duties performed.
- An adequate IT security training program.
- An adequate IT security management structure.
- Adequate physical access controls.
- Adequate IT systems contingency planning.

IT SYSTEMS SECURITY PLANS ARE NEEDED

The BOR had not developed individual IT system security plans for SCADA systems including the systems at the Hoover, Shasta, and Grand Coulee Dams operations. However, the Central Valley Operations office had prepared a draft security plan for its IT operations that included the Shasta Dam operations. The BOR should prepare individual IT systems security plans to provide an overview of the security requirements of each system and describe the controls in place or planned for meeting these requirements. In addition, each

²A firewall is a system or group of systems that enforces an access control policy between two networks.

plan should delineate responsibilities and expected rules of behavior of all individuals who access the systems. The BOR should follow the guidelines for preparing IT systems security plans described in the NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems." Additionally, the plans should be updated every 3 years or whenever significant changes are made to the IT systems.

Not having individual IT systems security plans that are administered and managed adequately could result in:

- Inadequate protection of information and technology resources.
- Not recognizing and adequately mitigating new risks.
- Lack of custodial accountability over information and technology resources.
- Unauthorized access and destruction of critical IT systems and resources.

Further, the lack of a security plan for each IT system should be reported to the Department as noncompliant with the Government Information Security Reform Act, the Computer Security Act, and the Office of Management and Budget (OMB) Circulars A-123, "Management Accountability and Control," and A-130, "Management of Federal Information Resources."

IT SYSTEM ACCREDITATION IS NEEDED

The BOR did not have documented policy and procedural guidance for ensuring that IT systems supporting energy and water operations were accredited (authorized to process by senior management) prior to being placed into operation or reaccredited when significant changes were made or at least every 3 years. Without having its IT systems accredited, the BOR was not in compliance with OMB Circular A-130, and the BOR would be required to report this deficiency to the Department.

IT SECURITY RESPONSIBILITIES NEED TO BE EXPLICITLY ASSIGNED

IT security responsibility over each of the IT systems was not specifically assigned. Consequently, the risk was increased that security products and techniques were not effective for safeguarding the BOR's critical IT systems and resources.

IT FIREWALL POLICIES AND PROCEDURES ARE NEEDED

The BOR installed firewalls to secure its IT systems without having formally approved policies and procedures that addressed firewall design. Firewall policies and procedures should address IT security concerns such as:

- Types of network services and resources that are allowed to be accessed by users (inside and outside of the BOR).
- Descriptions of business needs for the installation of a firewall, such as what IT resources are to be protected, the likelihood of threats, and the importance of the resources.
- Purposes of the firewalls: either to deny all traffic and services unless explicitly authorized or to authorize all traffic and services unless explicitly denied.
- Designate who is authorized to develop and authorize risk mitigation statements for each firewall.

The BOR should follow the guidelines for preparing firewall policies and procedures in the NIST Special Publication 800-10, "Keeping Your Site Comfortably Secured: An Introduction to Internet Firewalls."

Additionally, firewall administration had not been formally assigned to specific individuals for each of the BOR's installed firewalls. During the audit, the BOR designated a primary and a secondary firewall administrator for the firewalls located at the Hoover Dam and the Central Valley Operations office facilities and for the firewall for the Hydromet³ system.

Without policies and procedures that address network access, firewall design, and designated firewall administrators, the BOR was at risk that its firewalls may not be properly planned, may not be cost-effective security tools, and may not be configured to meet security needs to adequately safeguard networks and data from unauthorized access and manipulation.

IT INCIDENT HANDLING POLICIES AND PROCEDURES NEEDED The BOR did not have formal IT incident handling policies and procedures to ensure timely and efficient responses to IT security incidents if a computer virus, other malicious code, or a system intruder caused damage to systems and data or misused IT system resources. Further, the BOR's policies and procedures should ensure that evidence associated with an IT incident is safeguarded for use in potential legal proceedings.

No. 2002-I-0004 4

³Hydromet is a data collection system that provides water and weather-related data streams to a number of agencies, offices, and users within and external to BOR.

IT incident handling policies and procedures should address the definition of an IT security incident, procedures for protecting IT systems from incidents, a means for correcting the weakness that allowed an incident, and when an incident should be escalated for management attention or possible criminal investigation.

Without adequate IT security incident response policy and procedures, the BOR was at risk of not having the technical and procedural means to detect, mitigate, and appropriately report IT security incidents.

IMPROVEMENTS NEEDED IN DESIGNATING POSITION SENSITIVITY

The BOR personnel who had significant duties related to the operations of facilities and IT systems supporting energy and water operations did not have adequate position sensitivity designations and associated background clearances. In addition, periodic reinvestigations of these personnel were not conducted. For example, we found that positions for some IT security managers, SCADA managers and operators, and physical security officers were inappropriately designated nonsensitivenoncritical position sensitivity levels. This sensitivity designation is comparable to a low-risk public trust position designation. In addition, contracts that related to the power plants operations and IT systems did not include appropriate security clauses for contractor personnel. These contracts were for facilities maintenance, software development and maintenance, and janitorial services. We believe the BOR personnel and contractor positions that have duties related to IT and physical security, managing and operating SCADA systems, and developing and maintaining software should be designated as high-risk public trust positions. In addition, we believe that positions that are not designated high-risk but have duties related to maintaining and providing janitorial services for energy and water facilities should have access restricted and monitored.

Without appropriate position sensitivity designations or access restricted and monitored, the BOR has an increased risk of inappropriate employees or contractors having access to the systems and operations, which could result in the disruption of daily processes, manipulation of critical data, or extensive damage to the facilities and IT systems.

No. 2002-I-0004 5

IMPROVEMENT NEEDED IN IT SECURITY TRAINING

The BOR stated that computer security awareness training was available on the BOR intranet.⁴ However, we found no evidence that employees or contractors had taken security awareness training prior to being authorized access to the BOR IT systems and that employees and contractors had taken periodic security awareness training subsequent to being granted access to the BOR IT systems.

Without initial and periodic refresher training in IT security awareness and accepted IT security practices of employees and contractors who are involved in managing, using, or operating IT systems, the BOR's employees and contractors may not be aware of current IT security threats, vulnerabilities, and protective strategies.

IMPROVEMENT NEEDED IN IT SECURITY MANAGEMENT STRUCTURE

The BOR IT security manager position was three organizational levels below the BOR Chief Information Officer (CIO), and regional installation IT security personnel had not received adequate support from the BOR IT security manager. Further, at two of the seven sites we visited that had IT security managers, the IT security managers did not have authority to implement and enforce security policies and procedures and were not at the appropriate organizational levels.

The BOR had not ensured that the BOR IT security manager and regional installation IT security manager positions were at organizational levels commensurate with their IT security management responsibilities and were delegated sufficient authority to exercise their responsibilities. For example, the BOR IT security managers were not always able to:

- Review security policies and directives to ensure that IT resources were adequately safeguarded.
- Coordinate all activities designed to protect an IT installation or any other technical system.
- Provide technical assistance to program officials and managers on IT security requirements.
- Ensure IT security safeguards are included in contract specifications for the acquisition or operation of hardware, software development, or equipment maintenance services for the installation.

⁴An intranet is a network based on internet technology that belongs to an organization, usually a corporation, and accessible only by the organization's members, employees, or others with authorization.

Without an appropriate IT security management structure, the BOR had little assurance that its IT security program had effective controls and that implemented controls were reliable.

IMPROVEMENTS NEEDED IN PHYSICAL ACCESS CONTROLS

The BOR did not ensure that physical controls were effective in protecting energy and water facilities and supporting IT systems. For example, we found that:

- Access to power plants, switchyards, SCADA control rooms, and some computer rooms was not adequately controlled and monitored.
- Gates at Folsom and Keswick Dam facilities closed too slowly.
- Locks on the compound where the Boise satellite dishes were located were not tamper proof.
- Telecommunications equipment at the Northern California Area Office power plants could be easily accessed by anyone entering the power plants.
- The BOR wiring closets located in Building 67 on the Denver Federal Center were clearly identified as to their contents.
- There was no surveillance monitoring of the hallway that provided access to the BOR's computer room in Building 67.

When these physical control problems were discussed with the BOR, the following corrective actions were taken:

- The gate to the Keswick Dam facility was adjusted to close within 10 seconds after a vehicle passes through and cameras have been installed for monitoring access through the gate.
- The labels were removed from the BOR's wiring closet in Building 67.

In addition, corrective actions are being taken that when completed will improve physical access controls. However, the corrective plans have not been completed and do not include planned implementation dates.

Failure to adequately control access to protect facilities and IT systems increased the risk that the BOR's resources could be compromised or destroyed.

Although emergency action plans, which detail actions to be taken in the event of a disaster, existed for each energy and water operations facility, the plans did not include procedures for recovering IT systems, such as SCADA systems and local

IMPROVEMENTS NEEDED IN IT SYSTEMS RECOVERY CAPABILITIES

area networks. The BOR stated that one of the reasons that the plans did not include recovering IT systems was because the BOR's personnel would be able to physically perform the functions that are performed by the SCADA systems.

We also found that backups for the energy and water IT systems were not adequate and offsite storage facilities for backup tapes were not adequate or did not exist. For example:

- The Shasta Dam office did not regularly back up the computer operating system, which runs the SCADA system, and the SCADA application did not have an offsite backup storage facility, and the onsite storage facility was not environmentally controlled. During the audit, the BOR acquired an offsite storage facility to store the backup tapes.
- The Pacific Northwest Regional Office did not routinely store its backup of it servers at the offsite storage facility. In addition, the Office's offsite storage was not adequately secured or environmentally controlled. There was no official offsite storage facility for the Hydromet and AgriMet⁵ applications backup tapes (the tapes were kept at one employee's home).

Without adequate IT systems recovery capabilities, the BOR could not efficiently and effectively recover and resume its IT operations in the event of a system failure or a disaster.

RECOMMENDATIONS

We recommend that the Commissioner, BOR:

- 1. Report the deficient controls for an effective IT security management program, lack of security plans for each IT system, and lack of accredited IT systems as deficiencies to the Department for fiscal year 2001.
- 2. Ensure that the BOR CIO, in coordination with program managers, formally approves and implements comprehensive IT security policies and procedures that address security for IT systems supporting energy and water facilities and operations.

8

⁵AgriMet is a satellite-linked weather and evapotranspiration-reporting network. This network is used to assist irrigators in scheduling irrigation applications. Growers use the system's data along with field examinations to determine when and how much water is required for optimum crop growth. AgriMet is a subset of the overall Hydromet network.

- 3. Ensure that the BOR CIO, in coordination with program and regional managers, develops IT systems security plans for each IT system supporting energy and water facilities and operations. The security plans should be regularly updated to reflect significant changes to the environment or at least every 3 years.
- 4. Assign IT security responsibilities for each IT system supporting energy and water operations.
- 5. Ensure that IT systems supporting energy and water operations are accredited and re-accredited every 3 years or whenever significant changes are made to the IT systems.
- 6. Ensure that written policies and procedures are finalized, implemented, and maintained that address firewall design.
- 7. Ensure that firewall administration is specifically assigned to at least one primary and one secondary individual for each firewall installed.
- 8. Ensure that IT security handling policy and procedures are finalized, implemented, and maintained.
- 9. Ensure that sensitivity designations for positions related to supporting energy and water operations and supporting IT systems are appropriate based on an evaluation of position duties in relation to the magnitude of risk. For positions not designated high-risk access to facilities and IT systems should be restricted and monitored as appropriate.
- 10. Ensure that periodic reinvestigations are performed of employees who are in positions of high public trust.
- 11. Ensure that security clauses for contractor personnel are included, as appropriate, in contracts related to energy and water facilities and supporting IT systems. For contractor personnel positions that are not designated high-risk, ensure that access to facilities and IT systems is restricted and monitored as appropriate.
- 12. Formally approve and implement policies and procedures that ensure the BOR personnel and contractor personnel are provided IT security awareness training before access is granted to systems and refresher courses are completed and the attendance for each attendee is documented.

- 13. Elevate the BOR IT security manager position to report to the BOR CIO and ensure that the position has delegated authority to fulfill the position responsibilities.
- 14. Ensure that regional installation IT security managers do not report to individuals who are directly responsible for systems analysis, programming, equipment operation, or equipment maintenance and ensure that the positions are delegated authority to fulfill the position responsibilities.
- 15. Improve physical access controls to energy and water facilities and supporting IT systems. These access controls should ensure that the numbers of personnel with access to the power plants, switchyards, telecommunications equipment, and SCADA control rooms are limited to personnel whose duties require frequent access to these facilities and that access to facility computer rooms is monitored.
- 16. Develop, implement, and maintain, following the NIST guidelines, policies and procedures for IT systems continuity of operations planning that would ensure that an IT continuity of operations plan is developed for each system, the plans are periodically tested, and the plans are updated based on the test results.
- 17. Require that the BOR offices perform regularly scheduled backups for the IT systems.
- 18. Ensure that backup tapes are stored in appropriate environmentally controlled offsite and onsite facilities.

AGENCY RESPONSE AND OFFICE OF INSPECTOR GENERAL REPLY In the September 28, 2001 response to the draft report (Appendix 3), the BOR Commissioner concurred with the 18 recommendations. The Commissioner stated that BOR has increased the priority of its IT security management program and that significant resources have been provided to implement the policies, directives and standards, security mechanisms, and procedures to protect BOR assets. Several directives and standards have been implemented in response to our report including directives related to the development of security plans for national critical infrastructure systems and other IT systems, IT system security accreditation, IT security awareness training, physical access controls for the protection of BOR data and other IT resources, IT continuity of operations, and IT security incident handling response.

Accordingly, the Commissioner's response is sufficient to consider nine recommendations resolved and nine recommendations resolved but not implemented. The nine unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (Appendix 4). Further, recommendations classified as resolved will be examined during our fiscal year 2002 review of the DOI's compliance with the Government Information Security Reform Act.

The Commissioner's response also made specific comments on the draft report. These comments and our reply follow:

BOR COMMENTS. The Commissioner expressed concern that the scope of the audit was expanded from a review of the information technology (IT) critical infrastructure systems to IT systems supporting energy and water operations. Also, the Commissioner stated the scope expansion came without prior notice to the BOR. The Commissioner believed the original scope of the audit was expanded from reviewing "general controls over cyber-based energy and water infrastructure systems and related systems" to reviewing IT systems outside of the critical infrastructure sites (that is "information technology systems supporting energy and water operations").

OIG REPLY. The objective of the audit, which was clearly stated in our audit notification memorandum, was to determine the effectiveness of BOR's general controls over its cyber-based critical infrastructure systems and related systems. As explained at our entrance conference, this included not only the critical SCADA systems and any associated general support systems but also systems that serve the same purpose of supporting BOR's energy and water operations. We also advised at our entrance conference that other SCADA systems may be included in the review. As shown in Appendix 2, throughout the audit, other systems were reviewed. Prior to visiting these sites and reviewing the systems, we notified BOR CIO management of our plans. In addition, after each regional review was completed, our issues were discussed with regional staff and BOR CIO management. Therefore, we believe that BOR was fully aware of this audit activity.

DETERMINATION OF CRITICAL INFRASTRUCTURE SYSTEMS

Owners of Federal IT systems are required to develop adequate security controls in the areas of:

- Organization security policies and standards.
- Certified system security plans.
- Accredited IT systems.
- Documented and tested IT contingency plans.
- IT incident handling capabilities.
- IT security training program.
- Funding for IT security across the life cycle of each IT system.

We determined that the BOR did not have these controls for protecting its SCADA systems at the Hoover, Shasta, and Grand Coulee Dams.

If an IT system does not have all of the above controls and the Department has designated the system as a national critical infrastructure system, meaning that failure of the system would negatively impact the Nation, this deficiency must be reported as a material weakness to the Congress. The Department designated these three SCADA systems as national critical infrastructure systems.

The BOR disagrees with the Department's designation of these systems as national critical infrastructure systems. Because the BOR disagrees with the Department's designation of these systems and because proper asset valuations to value national critical infrastructures and systems were not performed, the Department's CIO and the OIG agreed that the deficiencies identified in this report would be reported to the Department as a deficiency for fiscal year 2001 rather than as a material weakness. However, if the systems are determined to be national critical infrastructure systems based on the asset valuations and if the deficiencies in this report are not corrected during fiscal year 2002, the Department will be required to report the fact that these SCADA systems do not have adequate security controls as a material weakness to the Congress.

RECOMMENDATION

We recommend that the Commissioner, BOR, ensure that asset valuations of the SCADA systems supporting the Hoover, Shasta, and Grand Coulee Dams energy operations be performed no later than September 30, 2002 to determine whether these systems should be designated as national critical infrastructure systems. The asset valuations should be performed using criteria

issued by the National Critical Infrastructure Assurance Office with input from the Department's CIO and the Department's Critical Infrastructure Assurance Office.

AGENCY RESPONSE AND OFFICE OF INSPECTOR GENERAL REPLY

In the September 28, 2001 response to the draft report (Appendix 3), the Commissioner, BOR concurred with the recommendation. The Commissioner stated that asset valuations of the designated national critical SCADA systems supporting the Hoover, Shasta, and Grand Coulee Dams energy operations would be conducted using guidance from the National Critical Infrastructure Assurance office and input from the Department.

Accordingly, the Commissioner's response is sufficient to consider the recommendation resolved but not implemented. This recommendation will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (Appendix 4).

AUDIT OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of this audit was to determine the effectiveness of the BOR's general controls over its water and energy critical infrastructure IT systems and related systems. The emphasis of the audit was on security controls that ensure integrity, confidentiality, authenticity, and availability of information and information systems.

We reviewed and tested the BOR's IT security management policies, procedures, and practices during fiscal year 2001 (January through July 2001) for safeguarding the BOR IT systems supporting energy and water operations. (See Appendix 2 for the BOR locations visited and the IT systems reviewed.)

Our audit was conducted in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included tests and other auditing procedures that were considered necessary under the circumstances.

Section 5(a) of the Inspector General Act (5 U.S.C. app. 3) requires the Office of Inspector General to list this report in its semiannual report to the Congress. In addition, the Office of Inspector General provides audit reports to the Congress.

This report is intended for the information of management of the Department of the Interior, Office of Management and Budget, and the Congress.

APPENDIX 1

Information Technology Criteria

DEPARTMENT OF THE INTERIOR (DOI)

The DOI Manual (375 DM 19), "Information Technology Security," states that bureau IT security manager positions "must be at an organizational level commensurate with the responsibilities assigned and must be delegated sufficient authority to exercise these responsibilities." This Manual section also states that installation IT security managers "shall not be, or report to, any individual who is directly responsible for systems analysis, programming, equipment operation, or equipment maintenance." Further, this Manual section requires that procedures for backing up and recovering data and software be included in IT contingency plans.

The DOI's, "Interim Network Perimeter Security Standard," describes elements that should be included in each firewall design policy including requirements for authentication, ports that will allow access, and the level of security over the "open" ports. In addition, the Standard includes procedures and methodologies to implement policy. Further, the Standard requires that for each firewall implemented at least one primary and one secondary firewall administrator be designated in writing.

The DOI Manual (441 DM 1-3), "Personnel Security and Suitability Requirements," requires that designation of a position be "at a level of risk based on the degree of damage that an individual, by virtue of the occupancy of the position, could do to the Federal service." This Manual section states that "high risk" positions include "those that have the potential for exceptionally serious impact involving duties especially critical to the agency or a program mission with broad scope of policy or program authority or *significant computer systems involvement....*" The Manual also states that for appropriate personnel "initial investigations and periodic reinvestigations are conducted commensurate with the position sensitivity and risk level." In addition, the Manual requires that "a clause/statement will be included in contracts/consultant agreements stipulating the risk/sensitivity level of the activities performed under the contract/agreement." The security officer, in coordination with Human Resources and the program manager, designates the sensitivity level of contract employees and the type of background investigations required.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

The NIST Special Publication 800-10, "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls," states that before purchasing or installing a firewall organizations should develop a network security policy and related security policies such as service access policy and a firewall design policy for each planned firewall. Further, this Publication describes procedures for maintaining the policies.

The NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," requires that adequate physical security be in place to protect systems, buildings,

and related supporting infrastructures. The Handbook emphasizes performing regular backup of automated applications and data and providing secure backup storage as part of a contingency plan. The Handbook also states that the offsite storage facility should be physically and environmentally protected to prevent unauthorized individuals from access and to protect data from heat, cold, or harmful magnetic fields.

The NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," states that if a security function lacks appropriate independence it may have minimal authority, few resources, and receive little management attention.

OFFICE OF MANAGEMENT AND BUDGET (OMB)

The OMB Memorandum 01-08, "Guidance on Implementing the Government Information Security Reform Act," states that "all programs will include procedures for detecting, reporting, and responding to security incidents, including notifying and consulting with law enforcement officials, other offices and authorities, and the General Services Administration's Federal Computer Incident Response Capability (FedCIRC)."

The OMB Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," requires mandatory training prior to granting access to an IT system and periodic refresher training to assure that users continue to understand and abide by the applicable rules of the system. The Circular requires controls to safeguard all information processed, transmitted, or stored in Federal automated information systems. Further, the Circular requires a contingency plan and periodic testing of the plan for the capability to perform the functions supported by the application in the event of failure of the automated support.

PUBLIC LAWS

The Computer Security Act of 1987 requires mandatory periodic training in computer security awareness and accepted computer security practices for employees who are involved in managing, using, or operating Federal computer systems.

The Government Information Security Reform Act assigns to each Program manager within a Federal agency the responsibility for:

- Adequately ensuring integrity, confidentiality, authenticity, availability, and nonrepudiation of information and information systems supporting operations and assets.
- Developing and implementing information security policies, procedures, and control
 techniques sufficient to afford security protections commensurate with the risk and
 magnitude of the harm resulting from unauthorized disclosure, disruption, modification,
 or destruction of information collected or maintained.
- Ensuring that an information security plan is practiced throughout the life cycle of each system.

APPENDIX 2

Bureau of Reclamation Offices Visited and Systems Reviewed

Office Name and Location **System Reviewed** Information Resources Services Denver, Colorado Technical Services Center Local area network (LAN) Denver, Colorado Prime and Secondary Programmable Master Hoover Dam Supervisory Control (SCADA) and LAN Lower Colorado Dams Facility Office Boulder City, Nevada Mid-Pacific Region LAN Sacramento, California Central Valley Operations Central Valley Acquisition Control System Sacramento, California ((CVACS)/ SCADA) and LAN Folsom Dam CVACS Folsom, California Northern California Area Office Shasta Lake City, California **CVACS** Shasta Dam Shasta Lake City, California Keswick Dam CVACS, Back-up SCADA, LAN, and wide Redding, California area network Trinity Dam **CVACS** Lewiston, California Lewiston Dam **CVACS** Lewiston, California Whiskeytown Dam **CVACS** Judge Francis Carr Powerplant Lewiston, California Spring Creek Debris Dam **CVACS** Redding, California Grand Coulee Dam **SCADA** Grand Coulee Power Office Grand Coulee, Washington Hydromet, Agrimet, and LANs Pacific Northwest Region Boise, Idaho Black Canyon Diversion Dam SCADA, LAN, and wide area network

No. 2002-I-0004

Emmett, Idaho

APPENDIX 3



United States Department of the Interior

BUREAU OF RECLAMATION Washington, D.C. 20240

D-5010

SEP 28 3001

MEMORANDUM

To:

Office of Inspector General

Attention: Director, National Information Systems Office

From:

John W. Keys, III

Commissioner

Subject:

Draft Audit Report on "Improvements Needed in Security Management of

John Keyr, TI

Information Technology Systems Supporting Energy and Water Operations,

Bureau of Reclamation" (A-IN-BOR-001-01-M)

The Bureau of Reclamation appreciates the opportunity to review and comment on the subject report. The findings and associated audit recommendations identified by the report will be addressed in the ongoing initiatives to improve Reclamation's Security Program. However, Reclamation is concerned that the scope of the audit was expanded from a review of the information technology (IT) critical infrastructure systems to IT systems supporting energy and water operations. This scope expansion came between the preliminary draft and the draft report without prior notice to Reclamation or additional audit work being performed.

The original scope of the audit was expanded from "general controls over cyber-based energy and water critical infrastructure systems and related systems" to a revised scope that includes IT systems outside of our critical infrastructure sites: i.e., "information technology systems supporting energy and water operations." The definition of "related systems" agreed to by both Office of Inspector General (OIG) auditors and Reclamation program staff was: Reclamation owned and operated supervisory control and data acquisition (SCADA) systems at locations associated with the critical infrastructure sites; systems that use data from SCADA systems at critical infrastructure sites; and general support systems, such as local area networks, supporting critical infrastructure sites.

The OIG and Reclamation engaged in an informal process that involved the use of Notifications of Potential Finding and Recommendations, followed by the review and discussion of the preliminary draft report. This process provided the opportunity to discuss and clarify potential findings and recommendations and ensure that the information presented was accurate and clear. It also provided the opportunity for Reclamation to involve key staff (including executives, managers, and operational and technical staff) in the process and begin to address and resolve issues identified in the proposed recommendations. The final discussion of the contents of the

preliminary draft of the report took place prior to the exit conference. The final draft version of the report with the change in scope was received after the exit conference.

2

In recent years Reclamation has increased the priority of its IT security management program. Millions of dollars have been provided for independent IT security assessments conducted by the National Security Agency (NSA). Sandia National Laboratories (SNL), and Javis Automation and Engineering Inc. The SNL and NSA assessments specifically addressed the security of the cyber-based control systems in our critical infrastructure facilities. Reclamation executive management has provided significant resources (including \$5 million in funding for fiscal year 2002) to implement the policies, directives and standards, security mechanisms, and procedures to protect Reclamation IT assets. Reclamation recognizes that the IT security controls cited in the draft report need to be applied to all major applications and general support systems and has established the following priorities: (1) developing a framework of policy, directives, and standards, (2) implementing a perimeter IT security architecture, (3) implementing controls at the critical infrastructure sites, (4) developing a prioritized list of other systems and developing a schedule to implement controls for major applications and general support systems, and (5) conducting internal reviews of IT security business practices to improve the implementation of the IT Security Program.

In light of the recent terrorist activity on the east coast, Reclamation's IT security program remains a high priority and executive management feels that the appropriate steps to improve the level of IT security in Reclamation are being taken.

Reclamation's responses to the specific recommendations follow. Please note that the responses to some of the recommendations cite compliance with the OIG's initial scope and identify implementation actions to address the OIG's revised scope.

Recommendation 1

Report the deficient controls for an effective IT security management program, lack of security plans for each IT system, and lack of accredited IT systems as deficiencies to the Department for fiscal year 2001.

Response

Concur. Reclamation will, upon receipt of the final audit report and the OIG's referral of the audit report to the Department of the Interior, report to the Department's Chief Information Officer the findings and recommendations of the audit and Reclamation's planned and completed actions related to the recommendations.

Target completion date for reporting to the Department is October 31, 2001. The responsible official is Reclamation's Chief Information Officer (CIO).

3

Recommendation 2

Ensure that the BOR CIO, in coordination with program managers, formally approve and implement comprehensive IT security policies and procedures that address security for IT systems supporting energy and water facilities and operations.

Response

Complied. Reclamation recognized the potential risks related to its IT security practices several years ago and contracted with consultants to assist with better defining those risks and recommending changes to improve IT security. Reclamation's CIO has worked with the Commissioner's Policy Team to develop and fund strategies for improving IT security Reclamation-wide. An IT security policy (attachment) establishing the framework for a Reclamation-wide IT Security Program was signed by the Commissioner in December 2000. Directives and standards have been developed and incorporated into the Reclamation Manual to address more specific aspects of IT security. Reclamation's IT Security Program: Audit and Systems Logging Directives and Standards address how implementation will be ensured.

Recommendation 3

Ensure that the BOR CIO, in coordination with program and regional managers, develops IT systems security plans for each IT system supporting energy and water facilities and operations. The security plans should be regularly updated to reflect significant changes to the environment or at least every 3 years.

Response

Concur. Reclamation's IT Security Program: IT System Security Accreditation Directives and Standards have been issued to ensure development of IT systems security plans for major and general support systems. These Directives and Standards include the requirement that plans be updated every 3 years or whenever significant changes are made to the system.

Based on the original scope of the audit, the target date for certification of the IT system security plans for SCADA systems at the critical infrastructure sites is January 1, 2002. The responsible officials for Shasta, Hoover, and Grand Coulee Dams are, respectively, the Directors, Mid-Pacific (MP) Region, Lower Colorado (LC) Region, and Pacific Northwest (PN) Region. The target date for completing a schedule for developing security plans for the remaining major applications and general support systems supporting energy and water facilities and operations is July 31, 2002. The responsible official is Reclamation's CIO.

Recommendation 4

Assign IT security responsibilities for each IT system supporting energy and water operations.

Response

Concur. Reclamation's IT Security Program: IT System Security Accreditation Directives and Standards have been issued to require the assignment of security responsibility for each major application and general support system in the IT system security plan.

Based on the original scope of the audit, the target date for certification of the IT system security plans (including designation of IT security responsibilities) for SCADA systems at the critical infrastructure sites is January 1, 2002. The responsible officials for Shasta, Hoover, and Grand Coulee Dams are, respectively, the Directors, MP Region, I.C Region, and PN Region. The target date for completing a schedule for developing security plans (including designation of IT security responsibilities) for the remaining major applications and general support systems supporting energy and water facilities and operations is July 31, 2002. The responsible official is Reclamation's ClO.

Recommendation 5

Ensure that IT systems supporting energy and water operations are accredited and re-accredited every 3 years or whenever significant changes are made to the IT systems.

Response

Concur. Reclamation's IT Security Program: IT System Security Accreditation
Directives and Standards require accreditation and authorization for operation of major
applications and general support systems (including those supporting energy and water
facilities and operations). These Directives and Standards also require that systems be reauthorized every 3 years or whenever significant changes are made.

Based on the original scope of the audit, the target date for accreditation of the SCADA systems at the critical infrastructure sites is January 1, 2002. The responsible officials for Shasta, Hoover, and Grand Coulee Dams are, respectively, the Directors, MP Region, LC Region, and PN Region. The target date for completing a schedule for accrediting the remaining major applications and general support systems supporting energy and water facilities and operations is July 31, 2002. The responsible official is Reclamation's CIO.

Recommendation 6

5

Ensure that written policies and procedures are finalized, implemented, and maintained that address firewall design.

Response

Complied. Reclamation's IT Security Program: Network Systems and Configuration Management of Security Mechanisms Directives and Standards define the requirements for security mechanisms, including firewalls. These Directives and Standards are being applied in the design of the IT security perimeter architecture and any other firewalls used in Reclamation. The internal review process defined in Reclamation's IT Security Program: Audit and Systems Logging Directives and Standards will ensure compliance with business practices.

Recommendation 7

Ensure that firewall administration is specifically assigned to at least one primary and one secondary individual for each firewall installed.

Response

Complied. As indicated in the draft audit report, primary and secondary firewall administrators have been designated for the three existing firewalls. In addition, Reclamation's IT Security Program: Network Systems Directives and Standards require that primary and secondary administrators be designated for each firewall installed.

Recommendation 8

Ensure that IT security (incident) handling policy and procedures are finalized, implemented, and maintained.

Response

Complied. An IT security policy establishing the framework for a Reclamation-wide IT Security Program was signed by the Commissioner in December 2000. IT Security incident handling procedures have been revised to provide Reclamation-wide consistency. In addition, Reclamation's IT Security Program: IT Intrusion Detection Systems and other directives and standards have been issued requiring use of those procedures for handling IT security incidents. A database has been established for incident tracking. The Bureau IT Security Manager and Regional IT Security Managers are tasked with implementation and maintenance of these procedures.

Recommendation 9

Ensure that sensitivity designations for positions related to supporting energy and water

6

operations and supporting IT systems are appropriate based on an evaluation of position duties in relation to the magnitude of risk. For positions not designated high-risk energy and water facilities and IT systems access should (be) restricted and monitored as appropriate.

Response

Concur. Reclamation will review positions related to IT systems supporting energy and water operations and, utilizing the guidelines in Departmental Manual, Part 441, will designate position sensitivity and risk level. As part of this review, Reclamation will survey the industry to determine common industry practice. Reclamation will also consider the relationship between sensitivity designations and access controls to ensure individuals in low-risk public trust positions do not have access to critical systems.

The target date for developing the position evaluation plan for positions related to supporting energy and water operations and supporting IT systems is July 31. 2002. This plan will include identification of responsibilities and training for those involved in the review process. The responsible official is the Director, Diversity and Human Resources Office.

Recommendation 10

Ensure that periodic reinvestigations are performed of employees who are in positions of high public trust.

Response

Concur. Reclamation recognizes the need for periodic reinvestigation of employees in positions of high public trust and will develop processes and procedures to ensure this is accomplished. The proposed procedures will be similar to existing procedures for reinvestigation of employees in positions of national security.

The target date for developing and distributing the reinvestigation processes and procedures is July 31, 2002. The responsible official is the Director, Diversity and Human Resources Office.

Recommendation 11

Ensure that security clauses for contractor personnel are included, as appropriate, in contracts related to energy and water facilities and supporting IT systems. For contractor personnel positions that are not designated high-risk, ensure that access to facilities and IT systems is restricted and monitored as appropriate.

Response

No. 2002-I-0004 22

7

Concur. Reclamation has developed standard clauses to be used in contracts involving access to systems supporting energy and water facilities and operations. These clauses will either limit or control access or require background investigations for contract personnel requiring unescorted access. As described in Departmental Manual, Part 441, processes will be established to screen, investigate, and manage these positions. Personnel involved in this process will be defined and trained to ensure that once the security clauses are placed in contracts, Reclamation has the ability to successfully fulfil the legal requirements of those clauses.

The target date for developing an implementation plan to address the sensitivity designation of contractor personnel accessing energy and water facilities and supporting IT systems is July 31, 2002. The responsible official is the Director, Operations.

Recommendation 12

Formally approve and implement policies and procedures that ensure the BOR personnel and contractor personnel are provided IT security awareness training before access is granted to systems and refresher courses are completed and the attendance for each attendee is documented.

Response

Complied. An IT security policy establishing the framework for a Reclamation-wide IT Security Program was signed by the Commissioner in December 2000. In addition, Reclamation's IT Security Program: IT Security Awareness and Training Requirements Directives and Standards have been issued stipulating IT security awareness training and refresher course requirements. A Web-based training course for IT security awareness has been available Reclamation-wide since March 2001. This course meets the mandatory requirements of OMB Circular A-130 and the Computer Security Act of 1987. In addition, it provides a mechanism for reporting completion of the training to the IT Security Officer and the local training officer. More than 1,600 people have completed the training since March 2001. Since it is Web-based, the training will be completed shortly after new employees or contractors have access to the intranet and before they have access to sensitive systems.

Recommendation 13

Elevate (Evaluate) the BOR IT security manager position to report to the BOR CIO and ensure that the position has delegated authority to fulfill the position responsibilities.

Response

Concur. Reclamation will evaluate the Bureau IT Security Manager position to ensure it has appropriate organizational responsibility, independence, technical resources, and authority. Reclamation separates the responsibility for applying IT security policy,

8

directives, procedures, and guidelines, which lies with the program managers and system owners, from the responsibility for the IT Security Program, which lies with the CIO.

The evaluation will be completed by March 31, 2002. The responsible official is Reclamation's CIO.

Recommendation 14

Ensure that regional installation IT security managers do not report to individuals who are directly responsible for systems analysis, programming, equipment operation, or equipment maintenance and ensure that the positions are delegated authority to fulfill the position responsibilities.

Response

Concur. Reclamation will evaluate the Regional IT Security Manager positions to ensure they have appropriate organizational responsibility, independence, technical resources, and authority and will move those positions within the organization as necessary.

The evaluation and realignment of positions if appropriate will be completed by March 31, 2002. The responsible official is Reclamation's CIO.

Recommendation 15

Improve physical access controls to energy and water facilities and supporting IT systems. These access controls should ensure that the numbers of personnel with access to the power plants, switchyards, telecommunications equipment, and SCADA control rooms are limited to personnel whose duties require frequent access to these facilities and that access to facility computer rooms is monitored.

Response

Complied. Reclamation has issued Reclamation's IT Security Program: Physical Access Directives and Standards to define the requirements for physical access controls related to IT systems. Reclamation has committed considerable resources to review and improve physical access controls for energy and water facilities and operations.

Recommendation 16

Develop, implement, and maintain, following the NIST guidelines, policies and procedures for IT systems continuity of operations planning that would ensure that an IT continuity of operations plan is developed for each system, the plans are periodically tested, and the plans are updated based on the test results.

Response

Complied. Reclamation has issued IT Security Program: Continuity of Operations (COO) Directives and Standards that define the requirements for COO planning and testing, as described in the NIST Special Publication 800-12 Guidelines. Facility COO Plans have been developed for each Reclamation site. Based on the original scope of the audit, IT appendices have been developed for the Hoover, Grand Coulee, and Shasta COO Plans. These plans and associated appendices prioritize the IT systems at each site and provide plans for continuity of system operations.

9

The target date for developing a schedule for completion of IT appendices to COO Plans for other energy and water facilities will be finalized by July 31, 2002. The responsible official is the Director, Operations.

Recommendation 17

Require that the BOR offices perform regularly scheduled backups for the IT systems.

Response

Complied. Reclamation's IT Security Program: System Backup Requirements Directives and Standards require Reclamation offices to perform regularly scheduled backups for IT systems.

Recommendation 18

Ensure that backup tapes are stored in appropriate environmentally controlled offsite and onsite facilities.

Response

Complied. Reclamation's IT Security Program: System Backup Requirements Directives and Standards require Reclamation offices to secure appropriate onsite and offsite storage facilities for backups. Reclamation's IT Security Program: Audit and Systems Logging Directives and Standards describe the mechanism for verifying that such procedures are followed.

Recommendation 19

We recommend that the Commissioner, BOR, ensure that asset valuations of the SCADA systems supporting the Hoover, Shasta, and Grand Coulee Dams energy operations be performed no later than September 30, 2002, to determine whether these systems should be designated as national critical infrastructure systems. The asset valuations should be performed using criteria issued by the National Critical Infrastructure Assurance Office with input from the Department's

10

CIO and the Department's Critical Infrastructure Assurance Office.

Response

Concur. Asset valuations of the SCADA systems supporting Hoover, Shasta, and Grand Coulee Dams energy operations are being conducted using guidance from the National Critical Infrastructure Assurance Office and input from the Department.

The target date for completion of the asset valuations of the SCADA systems at the critical infrastructure sites is January 1, 2002. The responsible officials for Shasta, Hoover, and Grand Coulee Dams are, respectively, the Directors, MP Region, LC Region, and PN Region.

Attachment

cc: Assistant Secretary - Water and Science, Attention: Olivia Ferriter

IRM PU1

Reclamati on Manual

Policy

Subject:

Reclamation Inform ation Technology Security Program

Purpose:

Defines and establishes authorities, principles, responsibilities, and accountability for Reclamation Inform ation Technology Security Program

Authority: The Privacy Act of 1974; Federal Managers' Financia Integrity Act of 1983, Public Law 100-235, The Computer Security Act of 1987; National Defense Authoriz ation Act for Fiscal Year 2001 (Subtitle G-Government Inform ation Security Reform); OMB Circular A-130, Appendix I.I. Security of Federal Automated Information Systems, OMB Circular A-123, Internal Control Systems CIAO Practices for Securing Critical Information Assets (January 2000); and Department of the Interior Departmental Manual Part 375 Chapter 19.

Contact:

Inform ation Resources Services, D-7100

Purpose. Reclamation's Inform ation Technology (IT) systems are a vital part of the infrastructure supporting the agency's mission of managing, developing, and protecting water and related resources in an environmentally and economically sound manner. These IT systems are protected from threats so that Reclamation can maintain and monitor contract obligations, safely and reliably operate facilities, and carry out mission-related administrative support responsibilities.

Definitions.

- A. Information Technology (IT). The equipment, interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by an executive agency. The term includes computers, ancillary equipment, software, firm ware and similar procedures, services (including support services), and related resources.
- B. IT Threat. A physical, electrical, or information-based hazard or compromise to an IT system or the communications, information, or control activities it performs or to which it is connected.
- Trusted. Confidence that an interfacing system, user, or network has met Reclamation requirements and will not compromise, corrupt, interrupt, change, or harm a Reclamation IT system or network. Untrusted means a lack of confidence, or of unknown confidence.

(128) 12/19/00 **NEW RELEASE** Page 1

IRM P01

Reclamati on Manual

Polic v

3. Goals and Objectives.

- A. Reclamation's IT Security Program will:
 - (1) Ensure the safety of personnel and the public.
 - (2) Protect the Federal investment.
 - (3) Take all reasonable and prudent precaution to prevent IT threats from detrim entally impacting mission effectiveness.
 - (4) Ensure the integrity of IT services to authorized project beneficianes by determining acceptable risk levels and by conducting periodic iT system audits to ensure compliance
 - (5) Provide for timely delivery of services via IT

4. Principles.

- A. Reclamation's Inform ation Technology Security Program (IT Security Program) incorporates security into the business practices and architecture of Reclamation's IT systems. The business requirement of protecting IT systems includes determination of acceptable risk and cost benefit analyses of alternative solutions. IT Security Program performance is measured to ensure IT system security cost-effectively supports Reclamation's mission.
- B. Electronic information is managed and protected as a Reclamation-wide asset. The 1T Security Program includes electronic Information Sensitivity Directives and Standards in order to support required assetmanagement and implement appropriate protective procedures.
- C The IT Security Program Incorporates efficient and effective Configuration Management Directives and Standards designed to ensure that system, procedural, organizational, physical, and personnel changes do not threaten IT system operations or increase vulnerabilities or risks.
- D The IT Security Program enforces a network security perimeter for IT systems as defined in the Network Systems Directive and Standard. These Directives and Standards identify the protective mechanisms to be implemented with trusted and untrusted systems and users.

(128) 12/19/00 NEW RELEASE Page 2

IRM PG1

Reclamati on Manual

Policy.

- E. IT security training and awareness is a Reclamation priority. The IT Security Program requires adequate IT security training for users, managers, IT technical personnel, and IT security personnel.
- 5 Scupe. This policy and the supporting Directives and Standards apply to:
 - All Reclamation-owned, -operated, and -maintained IT systems, including specialized systems (e.g., SCADA, Hydromet, GIS, Dam Safety).
 - All Reclamation-owned IT systems operated ang/or maintained by contract or temporary personnel
 - C. Ali Reclamation-owned IT systems operated and/or maintained by organizations or personnel other than Reclamation.
- 6. Responsibility/Accountability.
 - A. Reclamation's Chief Information Officer (CIO) is responsible and accountable for leading the IT Security Program and reports directly to the Commissioner of Reclamation.
 - B. Reclamation Directors, managers, and employees are responsible and accountable for ensuring systems are designed, implemented, and maintained in accordance with the IT Security Program Policies, Directors and Standards, and guidelines. Directors and managers are responsible for keeping the CIO adequately informed of IT Security Program issues, decisions, and accomplishments.
- 7. Supporting Directives and Standards. Recramation Manual Directives and Standards necessary to define the procedures and minimum mandated standards of practice for the IT Security Program will be developed in a collaborated process with input from affected managers and user communities and issued under the direction of Reclamation's CIO and included in the IRM section of the Reclamation Manual.

(128) 12/19/00 NEW RELEASE Page 3

APPENDIX 4

STATUS OF AUDIT REPORT RECOMMENDATIONS

Recommendation Reference	Status	Action Required
2, 6, 7, 8, 12, 15, 16, 17, and 18	Resolved.	No further response is required.
1,3, 4, 5, 9, 10, 11, 13, 14, and 19	Resolved, not Implemented.	No further response to the Office of Inspector General is required. The recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

NOTICE

This document is a final report of the Office of Inspector General. It is being made available to officials having responsibilities concerning the subjects discussed for their information or review and action.

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

Any questions regarding the use of this final audit report should be directed to the General Counsel's Office, Office of Inspector General, at (202) 208-4356.



Mission

The mission of the Office of Inspector General (OIG) is to promote excellence in the programs, operations, and management of the Department of the Interior (DOI). We accomplish our mission in part by objectively and independently assessing major issues and risks that directly impact, or could impact, the DOI's ability to carry out its programs and operations and by timely advising the Secretary, bureau officials, and the Congress of actions that should be taken to correct any problems or deficiencies. In that respect, the value of our services is linked to identifying and focusing on the most important issues facing DOI.

How to Report Fraud, Waste, and Abuse

Fraud, waste, and abuse in Government are the concern of everyone – Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or insular area programs and operations. You can report allegations to us by:

Mail: U.S. Department of the Interior

Office of Inspector General Mail Stop 5341-MIB 1849 C Street, NW

Washington, DC 20240

Phone: 24-Hour Toll Free 800-424-5081

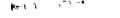
 Washington Metro Area
 202-208-5300

 Hearing Impaired
 202-208-2420

 Fax
 202-208-6023

Caribbean Region 703-487-8058 Northern Pacific Region 671-647-6060

Internet: www.oig.doi.gov/hotline_form.html





U.S. Department of the Interior Office of Inspector General

AUDIT REPORT

AUTOMATED LAW ENFORCEMENT SYSTEM, U.S. FISH AND WILDLIFE SERVICE

> REPORT NO. 97-I-1305 SEPTEMBER 1997



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

NOV - 3 1997

MEMORANDUM

TO: The Secretary

FROM: Wilma A. Lewis

Inspector General

SUBJECT SUMMARY: Final Audit Report for Your Information - "Automated Law

Enforcement System, U.S. Fish and Wildlife Service"

(No. 97-I-1305)

Attached for your information is a copy of the subject final audit report. The objectives of the audit were to: (1) determine whether the U.S. Fish and Wildlife Service's automated law enforcement system, the Law Enforcement Management Information System (LEMIS II), met the law enforcement reporting requirements of the Federal Bureau of Investigation and (2) provide information to the Service that would assist it in implementing LEMIS II effectively.

We found that LEMIS II is capable of meeting the law enforcement reporting requirements of the Federal Bureau of Investigation. However, improvements are needed to ensure that all crime statistics are reported and that law enforcement information is available to Service managers. Specifically, the Service needs to ensure that all elements of crime statistics required by the National Incident Based Reporting System (NIBRS) and the Department are included in the LEMIS II database, data input and edit controls are upgraded, and security over data is strengthened.

Based on the response from the Acting Director, U.S. Fish and Wildlife Service, we considered 2 of the report's 10 recommendations resolved and implemented, 3 recommendations resolved but not implemented, and 5 recommendations unresolved. We have asked the Service to reconsider its position on the five unresolved recommendations.

If you have any questions concerning this matter, please contact me at (202) 208-5745 or Mr. Robert J. Williams, Assistant Inspector General for Audits, at (202) 208-4252.

Attachment



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

SEP 3 0 1997

AUDIT REPORT

Memorandum

To: Assistant Secretary for Fish and Wildlife and Parks

Robert J. Williams Wobert J. Wieliams Assistant Inspector General for Audits From:

Subject: Audit Report on the Automated Law Enforcement System,

U.S. Fish and Wildlife Service (No. 97-I-1305)

INTRODUCTION

This report presents the results of our audit of the U.S. Fish and Wildlife Service's automated law enforcement system, the Law Enforcement Management Information System (LEMIS II). Our audit was conducted as part of our review of the Department of the Interior's automated law enforcement systems. The audit objectives were to: (1) determine whether LEMIS II met the law enforcement reporting requirements of the Federal Bureau of Investigation and (2) provide information to the Service that would assist it in implementing LEMIS II effectively.

BACKGROUND

The Service's law enforcement program provides protection for a broad spectrum of fish, wildlife, and plants through the application of a full range of law enforcement techniques, including: (1) surveillance of areas of fish and wildlife resources to prevent taking; (2) inspection of shipments arriving at and departing from designated borders and ports; and (3) enforcement of Federal regulations concerning protected species. enforcement program is a component of the Service's Refuges and Wildlife Activity. which is organized into seven regions. The law enforcement program is operated primarily through the Service's Division of Law Enforcement. The Division of Law Enforcement includes a Special Operations Branch, which conducts undercover operations of illegal takings and commercialization of wildlife, and Wildlife Inspectors, who monitor ports and borders for illegal imports and exports of protected species. In addition, the Division of Refuge Operations, through Refuge Officers, enforces Federal regulations on National Wildlife Refuges.

Under the Uniform Federal Crime Reporting Act of 1988 (Public Law 100-690), which became effective on January 1, 1989, the Congress mandated that all Federal agencies with law enforcement responsibility report crime statistics. In response to the Act, the Federal Bureau of Investigation requires that crime statistics be reported in a uniform computerized format to its automated system the National Incident Based Reporting System (NIBRS). The NIBRS program, which also became effective on January 1, 1989, and is defined in Volumes I-III of the "Uniform Crime Reporting National Incident-Based Reporting System" and in the "Supplemental Guidelines for Federal Participation," requires Federal agencies to submit, on a monthly basis, information on 22 offense categories for each crime investigated (the offense categories are in Appendix 1). The information to be reported includes the following: location of the crime; race, sex, and age of the offenders; information about the victims and property involved in the crime; and information on arrests, such as arrest date and type of apprehension. At the time of our review, the Department was reporting criminal investigation data under the Uniform Crime Reporting Program instead of NIBRS. The Program, which was the predecessor to NIBRS, requires summary information to be submitted monthly to the Federal Bureau of Investigation on the number of crimes investigated for only eight offense categories (see Appendix 1).

The Division of Law Enforcement manages the Service's automated law enforcement case management systems. The first automated system, the Law Enforcement Management Information System (LEMIS), was established in 1983. LEMIS was developed in-house; operated on a minicomputer; and designed so that users had direct access to the computer to add, change, delete, and query data. In 1991, the Service determined that since the hardware and software for LEMIS were obsolete and did not meet NIBRS requirements, a new system should be developed. Design and development of the new law enforcement system, LEMIS II, which was to replace LEMIS, began in 1991. LEMIS II was designed to accommodate NIBRS requirements, comply with the Department's reporting requirements for drug-related criminal activity, and satisfy the Service's specific information management needs. In that regard, LEMIS II will have five modules: investigations, permits and licenses, import/export declarations, skills inventory, and administrative. At the time of our review, only the investigations module was being implemented, and the other four modules were being developed. LEMIS II runs on a client/server, with a minicomputer functioning as the Data are entered into personal computers at regional and field sites and are electronically transferred to the server, where the Servicewide law enforcement database is maintained by the Division of Law Enforcement. The telecommunications network, which is used for the electronic transfer of data, is managed by the Division of Information Resources Management. Only after the data are uploaded into the database can managers and law enforcement agents from other offices perform queries on the data. The Service is operating LEMIS and LEMIS II simultaneously at those locations where LEMIS II has been implemented. LEMIS will continue to operate until LEMIS II is fully implemented Servicewide.

_

¹Client/server is a computerized architecture in which one or more "shared computers called servers manage shared resources and provide access to those shared resources as a service to their clients," which are personal computers that are used by individuals. David Vaskevitch, <u>Client/Server Strategies</u>, a <u>Survival Guide for Corporate Reengineers</u>, <u>IDG</u> Books Worldwide, Inc., San Mateo, California, 1993, page 96.

SCOPE OF AUDIT

To accomplish our objectives, we reviewed system documentation and interviewed management and staff at the Service's Division of Law Enforcement in Arlington, Virginia; regional offices in Lakewood, Colorado, and Atlanta, Georgia; the Division of Law Enforcement's Golden Field Office, in Golden, Colorado; and the Division of Information Resources Management, in Golden. Since the Service was replacing LEMIS with LEMIS II, we limited our audit scope to a review of the general and application controls and the system operations that had been implemented with LEMIS II.

Our audit was conducted in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances. As part of our review, we evaluated the system of internal controls to the extent that we considered necessary. The internal control weaknesses that we found are discussed in the Results of Audit section of this report. If implemented, our recommendations should improve the internal controls.

We also reviewed the Department of the Interior's Annual Statement and Report, required by the Federal Managers' Financial Integrity Act, for fiscal years 1994 and 1995 and determined that none of the reported weaknesses were directly related to the objectives and scope of this audit.

PRIOR AUDIT COVERAGE

During the past 5 years, the General Accounting Office has not issued any audit reports related to the Service's automated law enforcement system. However, in June 1989, the Office of Inspector General issued the report "Law Enforcement Activities, U.S. Fish and Wildlife Service" (No. 89-81), which stated that the Service's automated law enforcement system did not accurately record investigative time and did not adequately document and track all incidents. The report also stated that the Service had not adequately trained its system users. The report recommended that the Service ensure, in coordination with the Assistant Secretary for Policy, Budget and Administration (now the Assistant Secretary for Policy, Management and Budget), that a management information system was established which could track and provide uniform reports on cases and on productivity for Service law enforcement activities. The Service concurred with the recommendation and agreed to comply with guidance from the Office of the Secretary concerning this effort. In addition, in March 1993, the Office of Inspector General issued the report "Automated Data Processing Management, U.S. Fish and Wildlife Service" (No. 93-I-864), which stated that the Service was not in compliance with the Computer Security Act of 1987. The report recommended that the Service prepare risk analyses and contingency plans for all sensitive systems and software applications. Based on the Service's response, we considered the recommendation resolved and implemented.

RESULTS OF AUDIT

We concluded that the U.S. Fish and Wildlife Service's automated law enforcement system LEMIS II, is capable of meeting the law enforcement reporting requirements of the Federal Bureau of Investigation. However, improvements are needed to ensure that all crime statistics are reported and that law enforcement information is available to Service managers. Specifically, the Service needs to ensure that all elements of crime statistics required by NIBRS and the Department are included in the LEMIS II database, data input and edit controls are upgraded, and security over data is strengthened.

Data Elements

The Service did not ensure that all NIBRS and Departmental data elements were included in LEMIS II. Specifically:

LEMIS II included only 46 of the 52 reporting elements required by NIBRS. The Services justification for developing LEMIS II was to incorporate all of the required NIBRS elements into the Service's law enforcement system. Division of Law Enforcement officials said that six reporting elements were not included because the Service would not have any violations involving those elements. However, we found that for 1995 the Service had reportable data on seized and forfeited property, which was one of the elements not included in LEMIS II. In that regard, the Service's 1995 financial statements reported \$1.8 million of seized and forfeited property. The Service should include all the required reporting elements to ensure that the data transmitted to NIBRS are complete.

- LEMIS II included only 6 of the 19 management information items for law enforcement case files required by the Department. Service officials said that the 13 items did not have to be in the LEMIS II database because the information was maintained in hard copy in the case report files. However, in our opinion, if all 19 items are not included in LEMIS II, the effectiveness of maintaining an automated database management system is diminished.

Data Processes

The Service did not ensure that processes to input data into LEMIS II were effective and properly controlled. For example:

Division of Law Enforcement officials had planned for the Division of Refuge Operations law enforcement data to be input into LEMIS II. However, at the time of our review, notices of violations originating from the Division of Refuge Operations were not always entered into the LEMIS II database, and the Service had not determined who was responsible for ensuring that data would be entered into LEMIS II. Notices of violations that are issued by Refuge Officers for incidents pertaining to any of the 22 offense categories are required by the Act to be reported to NIBRS. For these incidents, the Refuge Officers prepare a manual report for their case files, and they can submit the report to a regional law enforcement office for input into LEMIS II. However, we found that the data were not always being entered into LEMIS II because the Service did not require Refuge Officers to

submit the reports to the regional law enforcement offices or require regional law enforcement officials to collect and enter data from the reports into LEMIS II. As an alternative, Division of Refuge Operations personnel could enter their law enforcement data directly into LEMIS II. However, the Division of Law Enforcement did not allow Division of Refuge Operations personnel to enter data directly into LEMIS II because of concerns over unauthorized access to sensitive data. We believe that LEMIS II could be programmed to restrict access to sensitive data and that Division of Refuge Operations personnel could enter their law enforcement data directly into LEMIS II.

In a related matter, Division of Refuge Operations officials said that the Division was planning a new automated system for their activity which will incorporate law enforcement information. However, before proceeding with this system, we believe that the feasibility of using LEMIS II for all law enforcement data processing should be determined.

- Division of Law Enforcement officials said that they had planned to have law enforcement agents input their own case and incident information into LEMIS II. However, the Service did not perform, as part of its system development life cycle management, analyses to determine the amount of time and effort required to input data when developing LEMIS II. During our review, regional managers said that they did not want law enforcement agents to perform the input function because of the amount of time needed to input the data. As such, the responsibility for input of the data was assigned to the legal assistants. According to the legal assistants, they also did not have enough time to input the data and perform their other duties. Consequently, data were not entered timely and completely into LEMIS II. Additionally, law enforcement agents and legal assistants used either LEMIS, Federal Bureau of Investigation systems, or hard copies in the files for querying and maintaining case and incident information rather than only LEMIS II, which we believe was not the most efficient use of resources. Therefore, an analysis should be performed by the Service to reduce the amount of time needed for Division of Law Enforcement and Division of Refuge Operations personnel to enter data into LEMIS II.
- When Division of Law Enforcement personnel electronically transmitted data from personal computers to the Servicewide law enforcement database, they did not receive notification that the data had been received and that the database had been updated. Because there was no notification, users had to perform queries to validate the information in the database. We believe that errors could be more readily identified and corrected and **staff time** used more efficiently if users were notified automatically that updates were accepted or that the data were rejected.
- The Service has not ensured that the data it will transmit to NIBRS will be accepted. At the time of our review, the Service had not coordinated with the Department or the Federal Bureau of Investigation to test the Service's data for acceptability into NIBRS. Therefore, there is no assurance that the Service's data will be included in the Federal Bureau of Investigation's NIBRS database.
- In addition, users were not adequately trained to fully operate LEMIS II, with the last training session for LEMIS held in 1994. The Division of Law Enforcement, in coordination with the Service's Division of Information Resources Management, developed a standardized

training program for the investigations module of LEMIS II. Each Regional Director was responsible for allocating resources for LEMIS II training. However, we found that the last training session was held in 1994 because Regional Directors had not been allocating the resources necessary to fund the training sessions.

Data Security

The legal assistants who input data into LEMIS and LEMIS II did not have the required security clearances. Because information contained in LEMIS and LEMIS II is sensitive and subject to the Privacy Act, system users are required by the Departmental Manual (446 DM 14.6 D) to have a background investigation and receive a security clearance. However, Service officials said that they did not require security clearances for the legal assistants because of the costs for these investigations. If legal assistants continue to input data into LEMIS and LEMIS II, they should receive the required clearances to ensure that sensitive data are adequately safeguarded.

Recommendations

We recommend that the Director, U.S. Fish and Wildlife Service, ensure that:

- 1. All NIBRS-required data elements are included in the LEMIS II database.
- 2. All the management information items of the law enforcement case files required by the Departmental Manual are included in LEMIS II.
 - 3. Law enforcement data for the Division of Refuge Operations are input into LEMIS II.
- 4. A feasibility study is performed to determine whether LEMIS II should be used for all law enforcement data processing.
- 5. Time frames are established for inputting accurate and complete data in a timely manner to LEMIS II to meet law enforcement program information needs and **NIBRS** reporting requirements.
- 6. Users are notified of successful or unsuccessful transmissions and updates to the Servicewide database.
- 7. The Division of Law Enforcement coordinates with the Department and the Federal Bureau of Investigation to test the Service's data transmitted to NIBRS.
- 8. **Regional** Directors allocate sufficient resources for training system users in how to use the modules and on the transmission and uploading processes.
- 9. Personnel who have access to LEMIS II have the appropriate security clearances based upon their duties and position sensitivity.

10. A waiver from the Office of Management and Budget for consolidation of agency data centers is requested or assurance is provided that the Service is complying with the requirements of Office of Management and Budget Bulletin 96-02.

U.S. Fish and Wildlife Service Response and Office of Inspector General Reply

In the March 27, 1997, response (Appendix 2) from the Acting Director, U.S. Fish and Wildlife Service, to our draft report, the Service agreed with Recommendations 2, 6, 7, and 8 and disagreed with Recommendations 1, 3, 4, 5, 9, and 10. Based on the response, we consider Recommendation 8 resolved and implemented; Recommendations 2, 6, and 7 resolved but not implemented; and Recommendations 1, 3, 4, 5, and 9 unresolved. Although the Service disagreed with Recommendation 10, it stated that its Division of Information Resources Management "completed a review of computer facilities nationwide in February 1996 and determined that no Service facilities met the definition of a 'data center' as prescribed by" Office of Management and Budget Bulletin 96-02. As such, we consider the recommendation resolved and implemented because the Service provided assurance that it has complied with Office of Management and Budget Bulletin 96-02. Accordingly, the unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation., and the Service is requested to respond to the unresolved recommendations, including revised Recommendation 5 (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service disagreed with the recommendation, stating that the "NIBRS elements excluded from the LEMIS II system pertain exclusively to tracking stolen property," that it "does not investigate crimes dealing with stolen property," and that "adding these elements to LEMIS would serve no purpose."

Office of Inspector General Reply. We disagree that the six data elements omitted pertain exclusively to tracking stolen property. Although five of the six data elements omitted relate to property data (date recovered, number of stolen motor vehicles, number of recovered motor vehicles, suspected drug type, and estimated drug quantity and type), we believe that the elements cover more than just stolen property offenses. According to the NIBRS edition of the Uniform Crime Reporting Handbook, Chapter 7, "Property Data," reporting of the data elements is required for offenses such as burglary, drug/narcotic offenses, fraud offenses, larceny, and stolen property offenses. In that regard, we believe that the Service had reportable data in at least one of the omitted data elements. Specifically, the Service's Budget Justifications for fiscal year 1997 stated that the Service seized about 17,000 pounds of marijuana in 1995, for which, in our opinion., the quantity and type of drug should have been reported as a drug/narcotic offense.

In addition, the Departmental Manual (446 DM 13.6) emphasizes that Departmental law enforcement systems should include the 52 data elements which the Federal Bureau of Investigation requires for crime statistics reported to NIBRS. In its response to

Recommendation 2, the Service stated that an analysis would be performed for the next generation of LEMIS II and at that time the management information items required by the Departmental Manual would be included in the redesign. To comply with the Departmental Manual, the Service should also include all required NIBRS data elements in LEMIS II. The Service is therefore requested to reconsider its response to this recommendation.

Recommendation 3. Nonconcurrence.

Service Response. The Service disagreed and stated that access to LEMIS II data is limited to Division of Law Enforcement employees. The Service further stated, "[a]llowing other Divisions to access LEMIS to input their own case information could risk the release of sensitive information, thereby compromising privacy issues and [the] safety of officers working in a covert capacity." According to the **Service**, the Division of Refuge Operations has developed the Law Enforcement Incident Reporting System (LEIRS), which has data that are compatible with LEMIS. The data from LEIRS will be downloaded into LEMIS to permit "complete Service file transmission of NIBRS data."

Office of Inspector General Reply. We agree that the information in LEMIS II is sensitive and should therefore be protected from misuse or unauthorized disclosure. However, we firmly believe that LEMIS II can be programmed to prevent other law enforcement personnel, such as Refuge Officers, from accessing the "sensitive" data of the Division of Law Enforcement. In its response, the Service emphasized the availability of resources as a reason for not concurring with the recommendation, yet it undertook actions to develop, operate, and maintain two systems which capture and report similar information and perform similar functions, including reporting NIBRS data. We firmly believe that this is not an efficient use of limited law enforcement resources. The Service is therefore requested to reconsider its response to this recommendation.

Recommendation 4. Nonconcurrence.

Service Response. The Service stated that because of data security requirements, the different missions of the Division of Law Enforcement and the Division of Refuge Operations, and available resources, the decision to have two separate systems was "sound." The Service further stated that "[l]aw enforcement activities on refuges are fundamentally different from those activities conducted by the Division of Law Enforcement" and that data security and confidentiality are "paramount when considering officer safety."

Office of Inspector General Reply. We agree that data security and confidentiality are essential when officer safety is considered. However, we firmly believe that LEMIS II can be programmed to prevent the improper accessing of "sensitive" data of the Division of Law Enforcement. The Service did not provide any specifics relating to the fundamental differences in the two divisions' law enforcement activities that would require separate systems. Notwithstanding fundamentally different activities, the systems perform similar functions, such as capturing NIBRS data and maintaining law enforcement case data as specified by the Departmental Manual. We strongly disagree that expending limited resources to develop, operate, and maintain two systems which capture and report similar information and perform similar functions, including reporting NIBRS data, was a sound decision. To the

contrary, the operation and maintenance of two separate systems is not an efficient use of limited resources. The Service is therefore requested to reconsider its response to this recommendation.

Recommendation 5. Nonconcurrence.

Service Response. The Service stated, "To provide investigative information to Service managers and employees, as well as outside interest, it is essential that data are entered into LEMIS II in a timely and accurate manner." The Service further stated that "each data element is reviewed to ensure that the information collected is relevant and necessary"; that "the information entered into LEMIS is essential"; that "[c]lerical employees are assigned these data entry duties"; and that "on rare occasions," Special Agents may input information into LEMIS II. The Service concluded in it response that it "does not believe an additional analysis is needed at this time."

Office of Inspector General Reply. We agree that the data which are input into LEMIS II are essential and should be entered into LEMIS II timely and accurately. The response stated that clerical employees are assigned these data entry duties; however, it did not address the issue of the amount of time required to input data into LEMIS II. Accordingly, we still believe that the timeliness of input needs to be addressed because, as stated in the report, the clerical staff said that they did not have enough time to input data and perform their other duties. As such, data were not entered timely and completely into LEMIS II. Consequently, we have revised the recommendation to focus on establishing time frames for inputting data into LEMIS II to meet law enforcement program information needs and NIBRS reporting requirements. Therefore, we request that the Service respond to the revised recommendation.

Recommendation 9. Nonconcurrence.

Service Response. The Service disagreed with the recommendation, stating that requiring "criminal background investigations on non-Special Agent personnel" is "overburdensome and unnecessary" because "[c]urrent clearance procedures require that all personnel, who have access to LEMIS data, pass a local police criminal history inquiry"; "[t]he Division has never experienced a breach of security since the inception of LEMIS 15 years ago"; and "[t]he \$3,700 cost of a single background investigation on data entry personnel cannot be absorbed within the Law Enforcement budget."

Office of Inspector General Reply. The Service did not indicate whether the criminal history reviews required for personnel who have access to LEMIS data were performed at the time of initial hire or periodically thereafter. Further, the Service indicated that non-Special Agent personnel do not need the required security clearances because no incidents have occurred since the inception of LEMIS and because of the cost involved. However, in its response, the Service repeatedly emphasized the sensitive nature of the information in LEMIS and the paramount importance of maintaining security and confidentiality. Moreover, based on the requirements of the Departmental Manual (375 DM, 441 DM, and 446 DM), non-Special Agent personnel, because of their access capabilities to enter, change, and delete law enforcement data and because of the sensitivity of data in

LEMIS and LEMIS II, may require at least a "Minimum Background Investigation" and may even require a more extensive "Limited Background Investigation" at initial hire and periodically thereafter. Therefore, we believe that required background investigations based on the sensitivity and risk associated with the program are necessary to ensure that management controls are in place to adequately safeguard LEMIS and LEMIS II data and to ensure that the Service is in compliance with the Departmental Manual. The Service is therefore requested to reconsider its response to the recommendation.

In accordance with the Departmental Manual (360 DM 5.3), we are requesting your written response to this report by November 17, 1997. The response should include the information requested in Appendix 3.

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations' and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of U. S. Fish and Wildlife Service personnel in the conduct of our audit.

REPORTABLE OFFENSE CATEGORIES

National Incident Based Reporting System

1. Homicide Offenses

Murder and nonnegligent manslaughter

Negligent manslaughter

Justifiable homicide

2. Sex Offenses, Forcible

Forcible rape

Forcible sodomy

Sexual assault with an object

Forcible fondling

3. Robbery

4. Assault Offenses

Aggravated assault

Simple assault

Intimidation

5. Burglary/Breaking and Entering

6. Larceny/Theft Offenses

Pocket-picking

Purse-snatching

Shoplifting

Theft from building

Theft from coin-operated machine or device

Theft from motor vehicle

Theft of motor vehicle parts or accessories

All other larceny

7. Motor Vehicle Theft

- 8. Arson
- 9. Bribery
- 10. Counterfeiting/Forgery11. Destruction/Damage/Vandalism of Property
- Drug/Narcotic Offenses

Drug/narcotic violations

Drug equipment violations

- Embezzlement
- 14. Extortion/Blackmail
- 15. Fraud Offenses

False pretenses/swindle/confidence game

Credit card/automatic teller

Machine fraud

Impersonation

Welfare

Wire fraud

16. Gambling Offenses

Betting/wagering

Operating/promoting/assisting gambling

Gambling equipment violations

Sports tampering

- 17. Kidnaping/Abduction
- 18. Pornography/Obscene Material
- 19. Prostitution Offenses

Prostitution

Assisting or promoting prostitution

20. Sex Offenses, Nonforcible

Incest

Statutory rape

- Stolen Property Offenses (receiving, etc.)
- Weapon Law Offenses

Uniform Crime Reporting Program

1. Homicide

Murder and nonnegligent manslaughter

Manslaughter by negligence

2. Forcible Rape

Rape by force

Attempts to commit forcible rape

3. Robbery

Firearm

Knife or cutting instrument

Strong-arm, hands, fists, feet, etc.

Other dangerous weapons

4. Aggravated Assault

Firearm

Knife or cutting instrument

Other dangerous weapons

Hands, fist, feet, etc.

5. Burglary

Forcible entry

Unlawful entry

Attempted forcible entry

6. Larceny - Theft (except motor vehicle)

7. Motor Vehicle Theft

Autos

Trucks and buses

Other vehicles

8. Arson

structural

Mobile

Other



United States Department of the Interior

FISH AND WILDLIFE SERVICE

Washington, D.C. 20240

ADDRESS ONLY THE DIRECTOR FISH AND WILDLIFE SERVICE

In Reply Refer To: FWS/ADM 12-03-019599

MAR 27 1997

Memorandum

To: Assistant Inspector General for Audits

From: And Director Director

Subject: Response to Office of Inspector General (OIG) Draft Audit Report - Automated

Law Enforcement System, U.S. Fish and Wildlife Service (A-IN-FWS-001-96)

We have reviewed the subject report dated February 19, 1997. The following are Service responses to the Draft OIG Audit Report which recommends that the Director ensure that:

Recommendation 1. All NIBRS-required data elements are included in the LEMIS II database.

Response: Disagree. NIBRS elements excluded from the LEMIS II system pertain exclusively to tracking stolen property. As the Service does not investigate crimes dealing with stolen property, adding these elements to LEMIS would serve no purpose.

Recommendation 2. All the management information items of the law enforcement case files required by the Departmental Manual are included in LEMIS II.

Response: Agree. However, these changes cannot be made to a database with existing data. In the near future, the Service will begin to analyze the LEMIS system with the intent of identifying the steps needed to design the next generation of this computer system. The items required by the Departmental Manual will be included in the redesign. The system analysis is expected to be completed by March 3 1, 1998. Responsible Official: Assistant Director, Refuges and Wildlife. Due Date: March 3 1, 1998.

Recommendation 3. Law Enforcement data for the Division of Refuge Operations are input into LEMIS II.

Response: Disagree. Access to LEMIS II data is limited to Division of Law Enforcement employees. The sensitive nature of investigations conducted and administered by Law Enforcement requires that information be provided strictly on a "need to know" basis. Allowing other Divisions to access LEMIS to input their own case information could risk the release of sensitive information, thereby compromising privacy issues and safety of officers working in a covert capacity.

The Law Enforcement Incident Reporting System (LEIRS) has been developed by the Division of Refuges to capture case information for Refuge personnel. LEIRS data are LEMIS compatible and will be downloaded to LEMIS to permit a complete Service file transmission of NIBRS data.

Recommendation 4. A feasibility study is performed to determine whether LEMIS II should be used for all law enforcement data processing.

Response: Disagree. For several reasons, including data security, the difference in missions, and availability of resources, Service managers made a conscious decision to maintain separate systems for the Division of Refuges and the Division of Law Enforcement. Law enforcement activities on refuges are fundamentally different **from** those activities conducted by the Division of Law Enforcement and there is no need to share in data processing. As stated above, the need to maintain security and confidentiality of law enforcement records is paramount when considering officer safety, particularly when covert investigations are conducted. The Service believes that the decision to keep the respective systems separate was sound.

Recommendation 5. An analysis is performed to determine the amount of time required to input the data into LEMIS II and responsibilities for inputting the data are assigned.

Response: Disagree. To provide investigative information to Service managers and employees, as well as outside interests, it is essential that data are entered into **LEMIS** II in a timely and accurate manner. Clerical employees are assigned these data entry duties. However, Special Agents may, on rare occasions, be required to input information. Prior to the development or enhancement of any subsystems contained in the law enforcement computer system, each data element is reviewed to ensure that the information collected is relevant and necessary. The LEMIS Steering Committee, comprised of top Law Enforcement managers, determined that the information entered in LEMIS is essential. Therefore, the Service does not believe an additional analysis is needed at this time.

Recommendation 6. Users are notified of **successful** or unsuccessful transmissions and updates to the Service wide database.

Response: Agree. The Service is currently working with Information Resources Management (IRM) personnel to address this design flaw. The National Communications Center (NCC) of IRM is developing a LEMIS for Windows system which will address this problem. A prototype of the Windows system has already been demonstrated. Installation of the system is expected to be completed by September 30, 1997. Responsible Official: Assistant Director, Refuges and Wildlife. Due Date: September 30, 1997.

Recommendation 7. The Division of Law Enforcement coordinates with the Department and the Federal Bureau of Investigation to test the Service's data transmitted to NIBRS.

Response: Agree. The Service will coordinate data transmission through the Department of the Interior. Responsible Official: Assistant Director, Refuges and Wildlife. Due Date: December 3 1, 1997.

Recommendation 8. Regional Directors allocate sufficient resources for training system users in how to use the modules and on the transmission and uploading processes.

Response: Agree. During FY 1996, a **LEMIS** help desk was established within the Service to provide timely telephone response to LEMIS users. In addition, a computer specialist has been hired to deal specifically with transmission and the uploading/downloading processes. This individual has conducted several training sessions in various locations and will continue to provide training as needed. Completed.

Recommendation 9. All personnel who have access to LEMIS II have the required security clearances.

Response: Disagree. The Service opposes the requirement of criminal background investigations on non-Special Agent personnel for the following reasons:

- (i) Current clearance procedure requires that all personnel, who have access to LEMIS data, pass a local police criminal history inquiry involving NCIC and SCOPE criminal files.
- (ii) The Division has never experienced a breach of security since the inception of LEMIS 15 years ago.
- (iii) The \$3,700 cost of a single background investigation on data entry personnel cannot be absorbed within the Law Enforcement budget.

The Service believes that to require more extensive background investigations on clerical personnel is overburdensome and unnecessary.

Recommendation 10. A waiver from the Office of Management and Budget for consolidation of agency data centers is requested or assurance is provided that the Service is complying with the requirements of Office of Management and Budget Bulletin 96-02.

Response: Disagree. In accordance with the requirements of OMB Bulletin 96-02, the Service's Division of Information Resources Management completed a review of computer facilities nationwide in February 1996 and determined that no Service facilities met the definition of a "data center" as prescribed by that Bulletin. Section (6)(b) of OMB96-02 states that "an agency data center is defined as any automated information processing operation with a standing staff of five or more full-time-equivalent employees... Applications programmers are not included in calculating "FTE employees."

4

The Law Enforcement computer support staff in Arlington is comprised of three computer specialists, only two of whom provide operational support for LEMIS. The other specialist is responsible for the management and operation of the Law Enforcement Local Area Network (LAN). OMB 96-02 also states that "Facilities that merely support LANs, files servers or desktop computers are not categorized as agency data centers." The Service does not consider the LEMIS facility to be within the OMB definition of a data center and, therefore, no waiver is required.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/ Recommendation Reference	Status	Action Required
1, 3, 4, and 9	Unresolved.	Reconsider the recommendations, and provide action plans that include target dates and titles of officials responsible for implementation.
2, 6, and 7	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
5	Unresolved.	Respond to the revised recommendation. If concurrence is indicated, provide an action plan that includes a target date and title of the official responsible for implementation. If nonconcurrence is indicated, provide reasons for the nonconcurrence.
8 and 10	Implemented.	No further action is required.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

Within the Continental United States

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240 Our **24-hour**Telephone HOTLINE
1-800-424-5081 or
(202) 208-5300

TDD for hearing impaired (202) 208-2420 or 1-800-354-0996

Outside the Continental United States

Caribbean Region

U.S. Department of the Interior Office of Inspector General Eastern Division - Investigations 1550 Wilson Boulevard Suite 410 Arlington, Virginia 22209 (703) 235-9221

North Pacific Region

U.S. Department of the Interior Office of Inspector General North Pacific Region 238 Archbishop F.C. **Flores** Street Suite 807, PDN Building Agana, Guam 96910 (**700**) 550-7428 or COMM 9-O11-671-472-7279





United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

JUL - 9 1999

AUDIT REPORT

Memorandum

To:

Assistant Secretary Land and Minerals Management

From:

Robert J. Williams Pobert J. Williams
Assistant Inspector General for Audits

Subject:

Audit Report on Implementation of Recommendations for Improving General

Controls Over the Automated Information System, Royalty Management

Program, Minerals Management Service (No. 99-I-628)

INTRODUCTION

This report presents the results of our audit of implementation of the recommendations contained in our March 1998 audit report titled "General Controls Over the Automated Information System, Royalty Management Program, Minerals Management Service" (No. 98-I-336). The objective of our current audit was to determine whether the Minerals Management Service's Royalty Management Program satisfactorily implemented the recommendations made in our March 1998 report and whether any new recommendations were warranted. This audit supports the Office of Inspector General's opinion on the financial statements of the Minerals Management Service by evaluating the reliability of the general controls over computer-generated data that support the Royalty Management Program's portion of the financial statements.

BACKGROUND

The Minerals Management Service's Royalty Management Program is responsible for collecting and disbursing revenues of about \$4 billion annually that are generated from leasing Federal and Indian lands and for collecting royalties on minerals extracted from leased lands. To aid in accomplishing its mission objectives and meeting its financial reporting requirements, the Program uses an automated information system that includes a mainframe computer, a minicomputer, and personal computers and servers which support an enterprisewide network.¹ For collecting rents and royalties, the Program uses primarily the mainframe computer. For disbursing rents and royalties, verifying collections, and reporting financial information, the Program uses all of the components of its automated information system. The Program's automated information system was operated and maintained by a contractor.

Overall system security policies for the Program are established by the Installation Information Technology Security Manager, within the Program's Systems Management Division. The contractor is responsible for providing system security administration for the mainframe computer, the minicomputers, and the enterprisewide network.

SCOPE OF AUDIT

This audit was conducted during September through November 1998 at the Royalty Management Program's Systems Management Division, located in Lakewood, Colorado. The scope of our audit included an evaluation of the actions taken by Program management to implement the 23 recommendations made in our March 1998 report and reviews of the general controls in place during fiscal year 1998. To accomplish our objective, we interviewed Program and contractor personnel, reviewed system documentation, and reviewed and tested implementation of the recommendations contained in the March 1998 report.

The audit was conducted in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we evaluated the Program's general controls over its automated information system that could adversely affect the data processing environment. Because of inherent limitations in any system of internal controls, losses, noncompliance, or misstatements may occur and not be detected. We also caution that projecting our evaluations to future periods is subject to the risk that controls or the degree of compliance with the controls may diminish.

RESULTS OF AUDIT

Regarding the March 1998 report's 23 recommendations, we found that the Royalty Management Program had satisfactorily implemented 20 recommendations. Three recommendations (Nos. D.1, D.2, and G.1) were considered resolved but not implemented based on actions to be taken by the Program. Appendix 2 lists all of the prior report's

¹ Servers are computers that provide services to client computers on a network. Enterprisewide networks are networks that result when all the networks in a single organization are connected. (Jerry Fitzgerald and Alan Dennis, <u>Business Data Communications and Networking</u>, 5th edition, John Wiley & Sons, Inc., 1996.)

recommendations, the status of the recommendations, and actions taken to implement the recommendations. The actions taken on the recommendations have improved the general controls in the areas of security program, access controls, software development and change management, separation of duties, system software controls, and service continuity.

To further strengthen the general controls, we found that improvements were needed in the areas of access controls, security planning, and continuity of operations. Office of Management and Budget circulars and National Institute of Standards and Technology publications require Federal agencies to establish and implement computer security and management and internal controls to improve the protection of sensitive information in the computer systems of executive branch agencies. Program management did not ensure that (1) computer security training was received by employees and contractor personnel and access to computer processing was limited, (2) security plans were updated appropriately, and (3) disaster recovery plans were developed in compliance with established criteria. As a result, there was an increased risk of (1) unauthorized access to, modification of, and disclosure of sensitive data; (2) ineffective security planning; and (3) loss of system availability.

Overall, we identified four weaknesses and made four new recommendations for improving general controls at the Program. We do not consider these weaknesses to be a material weakness under provisions of the Federal Managers' Financial Integrity Act. A summary of the weaknesses in the areas of access controls, security planning, and continuity of operations is provided in the paragraphs that follow, and the weaknesses and our respective recommendations are detailed in Appendix 1.

Access Controls

We found weaknesses in access controls over the Program's automated information system. These weaknesses were in the areas of computer security training and logical access controls over computer processing. As a result, there was an increased risk that proprietary data maintained on the automated information system were vulnerable to unauthorized disclosure and manipulation, as well as an increased risk of disruption of service to users. We made two recommendations to address these weaknesses.

Security Planning

We found a weakness in the development and maintenance of security plans for sensitive systems. As a result, the security plans in place did not ensure that controls were established to protect information processed, transmitted, or stored in the general support system,² and there was an increased risk that the most appropriate and effective controls would not be

²Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," defines a general support system or system to mean "an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people."

identified and implemented by the Program. We made one recommendation to address this weakness.

Continuity of Operations

We found that the communication networks, which were part of the Program's general support system, were not included in the Program's disaster recovery plans. As a result, there was an increased risk that the communication networks may not be recovered in the event of a disaster. We made one recommendation to address this weakness.

Minerals Management Service Response and Office of Inspector General Reply

In the May 25, 1999, response (Appendix 3) to our draft report from the Director, Minerals Management Service, the Service concurred with the four recommendations. Based on the response, we consider Recommendations A.1 and B.1 resolved and implemented and Recommendations C.1 and D.1 resolved but not implemented. Accordingly, the unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (see Appendix 4).

Regarding our March 1998 report, the Service, in its May 1998 response, concurred with our classification of the prior recommendations, and we considered 20 of the 23 recommendations resolved and implemented and the remaining 3 recommendations (Nos. D.1, D.2, and G.1) resolved but not implemented. Accordingly, updated information on the status of the three prior unimplemented recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget (see Appendix 5).

Since the recommendations contained in this report are considered resolved, no further response to the Office of Inspector General is required (see Appendix 4).

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Service personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

ACCESS CONTROLS

A. Computer Security Training

Condition:

The Program's policy that required periodic computer security training of employees and contractor personnel to reduce the risk of disclosure of proprietary data had not been effectively implemented. We statistically tested 49 of the 717 employees who had access to the server component of the automated information system. We found that 28 of the 49 employees had not received periodic training in the protection of proprietary data. From our test results, we projected that of the 717 employees, 410 employees had not been trained recently in the protection of proprietary data. In addition, Program management did not ensure that contractor personnel received such training.

Criteria:

The Program's policy regarding data protection states that the Royalty Management Program will "rely on employee training, clearances, and physical controls as its primary means of protecting proprietary information." This policy also states that "all employees and contractors are required to protect proprietary information and receive periodic training regarding the protection of proprietary information."

Cause:

There were no controls in place to ensure that employees and contractor personnel received the training specified by Program policy.

Effect:

Since training was one of the Program's primary controls to protect against disclosure of proprietary data and this control had not been effectively implemented, there was an increased risk of unauthorized disclosure of proprietary data.

Recommendation:

We recommend that the Director, Minerals Management Service, implement procedures to ensure that all employees and contractor personnel receive periodic training on the protection of proprietary data as defined by Program policy.

ACCESS CONTROLS

B. Access Controls Over Computer Processing

Condition:

Access controls over the processing performed on the mainframe computer were inadequate. Specifically, we identified 171 individuals who had update access to the emergency libraries. Emergency libraries can contain changes to the production application programs that are used to process data to determine the distribution of royalties. By running a program from the emergency library, change control procedures are bypassed, and the risk is increased that an inappropriate program would be run which could adversely affect the Program's data.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. The Circular also requires agencies to implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The Circular further defines "adequate security" as "security commensurate with the risk and the magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information." In addition, the current Program policy addressing data protection states that the Program "applies the concept of 'least privilege' to protect the integrity of official records. Only those persons with the responsibility for adding, deleting, or modifying records are given update privileges."

Cause:

Program security administration personnel had established a group within the mainframe computer security software that included all Time Sharing Option² (TSO) users and had given this group update access to the emergency

¹"A library is a collection of programs or data files for a particular purpose." (Alan Freedman, <u>The Computer Glossary</u>, 4th edition, AMACOM Division of the American Management Association, 1989, p. 401.)

²Time Sharing Option is a software "that provides interactive communications for IBM's MVS [Multiple Virtual Storage] operating system. It allows a user or programmer to launch an application from a terminal and interactively work with it." MVS is the operating system used on IBM mainframes. "MVS is a batch processing-oriented operating system that manages large amounts of memory and disk space. Online operations are provided with CICS [Customer Information Control System], TSO and other system software." (Computer Desktop Encyclopedia, Version 9.4, 4th quarter, 1996, The Computer Language Company, Inc.)

ACCESS CONTROLS

libraries, even though all users with access to TSO were not authorized to perform updates to the emergency libraries. Although Program management relied on reviews by personnel responsible for managing changes and updates to the emergency libraries to detect any inappropriate activities, we believe that a more effective control would have been to reduce the possibility of inappropriate activities by limiting access.

Effect:

There was an increased risk that unauthorized changes to the mainframe applications in the production environment could occur, which could result in possible corruption³ and loss of data, as well as disruption of service to users. However, during our fieldwork, the Program eliminated the update access to the emergency libraries that was provided to all TSO users.

Recommendation:

We recommend that the Director, Minerals Management Service, establish policies and procedures to ensure that default accesses established in the automated information system provide access only to authorized users requiring such access.

³Corruption is the unauthorized altering of data or programs resulting in erroneous software logic. (Alan Freedman, <u>The Computer Glossary</u>, 4th edition, AMACOM Division of the American Management Association, 1989, p. 159.)

SECURITY PLANNING

C. Security Plans

Condition:

The security plans for sensitive systems referred to in the Program's "Automated Information Systems Security Plan," dated January 1998, did not reflect the current information technology environment at the Program. Specifically, the "IBM Security Plan" and the "DEC/VAX [Digital Equipment Corporation/Virtual Address Extension] Security Plan" were dated 1996. The IBM plan did not reflect the hardware platform that was implemented in 1997. Further, both of the plans identified the Outer Continental Shelf Information System (OCSIS) as a source of production information, but OCSIS had been replaced by the Technical Information Management System. Also, the "RMP Desktop 1997 Security Plan" identified the Resource Access Control Facility (RACF) and the System Management Facility (SMF) as the audit and variance detection controls in place. However, both RACF and SMF were in place on the mainframe, but the Royalty Management (RMP) Desktop application was a client/server system that used different audit and variance detection controls.

Criteria:

The Computer Security Act of 1987 requires the development of a security plan for each Federal computer system that contains sensitive information. The Act further states, "Such plan shall be revised annually as necessary." Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires that security plans be developed for each general support system. In addition, the Departmental Manual (375 DM 19) requires that security plans be prepared for new or significantly changed systems.

Cause:

Program management updated only the plans that were referred to in the Program's "Automated Information Systems Security Plan" every 3 years regardless of whether changes had occurred. In addition, Program management did not ensure that the Program's security plans accurately reflected the security controls of the Program's sensitive systems components.

Effect:

Security plans for the Program did not ensure that controls were established to protect information processed, transmitted, or stored in the general support system, and there was an increased risk that the most appropriate and effective general controls would not be identified and implemented by the Program. During our fieldwork, Program security management revised the

SECURITY PLANNING

IBM plan, "Mainframe - 1998 Security Plan," to reflect the current mainframe environment.

Recommendation:

We recommend that the Director, Minerals Management Service, ensure that security plans which are referred to in the Program's annual "Automated Information System Security Plan" accurately reflect the controls in place and are updated to reflect significant changes to the current information technology environment.

CONTINUITY OF OPERATIONS

D. Disaster Recovery Plans

Condition: Communication networks, which are part of the Program's general support

system, used by the Program's divisions that maintain proprietary and financial data were not included in the Program's disaster recovery plans.

Criteria: Office of Management and Budget Circular A-130 requires that the security

plan for a general support system address continuity of operations. The Circular states, "Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the

system. Manual procedures are generally NOT a viable back-up option."

Cause: Program management had not completed the Program's disaster recovery

plan for its communication network environment.

Effect: If the disaster recovery plans are incomplete because components of the

general support system are not included, personnel required to perform the disaster recovery procedures may not be able to recover critical systems in

the event of a disaster or a system failure.

Recommendation:

We recommend that the Director, Minerals Management Service, ensure that disaster recovery plans are developed for the general support system, including communication networks necessary to maintain Program operations.

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR AUDIT REPORT "GENERAL CONTROLS OVER THE AUTOMATED INFORMATION SYSTEM, ROYALTY MANAGEMENT PROGRAM, MINERALS MANAGEMENT SERVICE" (No. 98-I-336)

Recommendations

Status of Recommendations and Corrective Actions

- A.1. Ensure that risk assessments are conducted in accordance with guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the assessments should address significant risks affecting systems, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of the residual risk.
- A.2. Formally assign and communicate responsibility to local area network administrators to participate in risk assessments and ensure compliance with the Program's security policy.
- A.3. Determine the risks associated with local area network applications and personal computer databases which contain proprietary and financial data and, based on the results of the risk assessments, establish appropriate security policies and procedures.

Implemented. We found that the Royalty Management Program had implemented an enhanced risk assessment process which should identify the significant risks affecting the Program's automated information system, identify controls implemented to mitigate those risks, and formalize the acceptance of the residual risk. We believe that establishment of this process meets the intent of the recommendation.

Implemented. The Program had centralized the administration of its networks and established a team to ensure compliance with the Program's policy regarding risk assessments.

Implemented. The Program had performed an assessment of risks related to proprietary data and its official financial records. As a result of the assessment, the official records had been moved from personal computer databases to networks. Therefore, the proprietary and official financial records are subject to the controls established for the networks.

Recommendations

Status of Recommendations and Corrective Actions

B.1. Evaluate Systems Management Division and contractor automated data processing (ADP) positions to determine position sensitivity in relation to risk and ADP factors. Also, assurance should be provided that automated information system work is technically reviewed by persons whose position sensitivity levels are greater than the position sensitivity levels of the employees who are performing the work.

Implemented. The Program had evaluated Systems Management Division and contractor ADP positions to determine position sensitivity in relation to risk and ADP factors. Through the evaluation process, the sensitivity levels of Systems Management Division management and supervisory positions and contractor management positions were increased.

Status of Recommendations and Corrective Actions

Recommendations

B.2. Establish controls to ensure that the contractor is fulfilling its contractual obligation of submitting requests for background checks within the specified time frame and that contractor employees who are in probationary status and awaiting security clearances are not performing critical ADP work.

Implemented. A process was implemented in which the contractor provided a report containing the names of newly hired personnel working on the Program's contract, along with the submission status of the background check documentation. This report was used by the Program's security management and the Minerals Management Service's Personnel Division to ensure compliance with contract requirements regarding the submission of background check documentation. Also, the Program approved the contractor's implementation of a "pre-employment/preassignment screening" process. This process, which includes a criminal history review, credit check, and a driving history check, provides assurance to the Program that the contractor's potential employees would receive the appropriate security clearance. This procedure was implemented in lieu of not allowing contractor employees who are on probationary status and awaiting their security clearances to perform critical ADP work because the time required to obtain a security clearance is not cost beneficial to the Program. We believe that the contractor's alternative "preemployment/pre-assignment screening" process meets the intent of the recommendation.

Recommendations

Status of Recommendations and Corrective Actions

B.3. Establish controls to ensure that personnel or security files accurately reflect that background checks and periodic followup background checks are performed as required.

Implemented. Program background check information was being tracked by the Service's Personnel Division for Program and contractor personnel instead of requests for background checks being submitted through the Program's security personnel. In addition, Program management had taken action to submit required documentation for periodic followup background checks.

C.1. Establish controls to enforce Program policy that requires employees to sign security awareness statements before access to system resources is approved by the Installation Automated Information System Security Officer.

Implemented. The controls were established and enforced.

D.1. Ensure that individual computer resources are classified based on the level of sensitivity associated with each resource.

Resolved; not implemented. Although Program management did not agree with the recommendation in its response to our March 1998 audit report, we believe that the Program's risk management process implemented under Recommendation A.1 will require the Program to classify its individual computer resources based on the level of sensitivity associated with each resource. Therefore, we believe that completion of the revised risk assessments, which the Service said will occur by the end of calendar year 1999 using the new risk management process, will meet the intent of the recommendation.

Recommendations

Status of Recommendations and Corrective Actions

D.2 Evaluate controls over resources to ensure that the access controls have been implemented commensurate with the level of risk and sensitivity associated with each resource.

Resolved; not implemented. Although Program management did not agree with the recommendation in its response to our March 1998 audit report, we believe that the Program's risk management process being implemented under Recommendation A.1 will require the Program to evaluate its controls over its resources to ensure that the access controls have been implemented commensurate with the level of risk and sensitivity associated with each resource. Therefore, we believe that completion of the revised risk assessments, which the Service said will occur by the end of calendar year 1999 using the new risk management process, will meet the intent of the recommendation.

E.1. Implement controls to enforce Program policy that default user identifications (IDs) and passwords are removed from the automated information system when commercial off-the-shelf software is implemented.

Implemented. Program management issued a memorandum reaffirming the Program's policy, and a procedure requiring assurance of deletion/revocation of the default password was implemented.

Status of Recommendations and Corrective Actions

Recommendations

F.1. Evaluate the current Program policy which recommends that passwords contain a mix of letters and numbers for all automated information system components. Implement, if the Program determines that a mix of letters and numbers should be required, the security software option within RACF (Resource Access Control Facility) that would enforce this requirement. If the Program determines that a mix of letters and numbers is not required, the risk should be addressed in the risk assessment.

Implemented. The Program evaluated the current policy. As a result of the evaluation, the Program implemented a control within the mainframe environment requiring the use of passwords containing a mix of letters and numbers.

- F.2. Develop and implement centralized security administration for the local area networks used by the Program's divisions that contain proprietary and financial data.
- Implemented. The Program consolidated its servers and centralized security administration for its local area networks that contain proprietary or financial data.
- G.1. Implement controls to ensure that access managers approve all access to their applications in accordance with Program policy.
- Partially implemented. The Program made significant progress in completing its review of user access levels; however, the September 30, 1998, target date for implementation of this recommendation was changed to June 30, 1999.
- G.2. Document procedures which require that users' access levels be reviewed periodically or that employees be recertified to ensure that the levels of access granted are appropriate for the duties assigned to the users.
- Implemented. Procedures were documented, and the Program had begun to review user access levels cited in Recommendation G.1.

Recommendations

Status of Recommendations and Corrective Actions

H.1. Evaluate the need to deviate from the Department of the Interior standard for the number of unsuccessful log-in attempts. If the Program determines that this number should remain at five, Program management should request, from the Department, a waiver from the standard of three attempts.

Implemented. The Department's Office of Information Resources Management provided a waiver to the Program allowing the program to deviate from the standard pertaining to the number of log-in attempts.

I.1. Enforce procedures for authorizing, approving, and testing client/server applications software before the software is moved into production.

Implemented. The Chief, Systems
Management Division, issued a
memorandum reinforcing the established
procedures, and a monitoring officer was
designated to ensure compliance with the
standards on all new client/server projects.

J.1. Implement controls to ensure that application programmers do not have access to the production client/server application data or the capability to update/change these data.

Implemented. Controls were established to provide only temporary access in cases in which application programmers need to access production data and to promptly terminate this access when it is no longer required.

J.2. Improve detection controls by ensuring that management or the Installation Security Officer periodically reviews server security log files.

Implemented. Procedures were developed and implemented requiring periodic reviews of server security logs by security administration personnel.

K.1. Ensure that the upgraded version of RACF is implemented immediately if the Program is granted a waiver from consolidating its mainframe operations with another mainframe operation.

Implemented. The upgraded version of RACF was implemented.

Recommendations

Status of Recommendations and Corrective Actions

L.1. Evaluate acquiring system verification and auditing software.

L.2. Implement the system options to record activities in the system log (SYSLOG) during the system initialization process and develop and implement procedures to ensure that periodic reviews of the SYSLOG for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Program management.

L.3. Evaluate the available System
Management Facility (SMF) record types
and implement procedures to ensure that
critical SMF log files are reviewed
periodically and that Program management
addresses the problems identified.

M.1. Update the disaster recovery plans to include all mission-critical systems.

Implemented. The Program completed an evaluation of system verification and audit software and purchased a software tool to be used in its network environment that would include the mainframe.

Implemented. In fiscal year 1998, the Program implemented system options to record activities in the SYSLOG during the system initialization process and developed and implemented procedures requiring periodic reviews of the SYSLOG for unauthorized or inappropriate activities and requiring that such activities be reported to Program management. However, during this audit, we noted that the system logging option was disabled. After we informed Program management of this deficiency, the system logging option was turned back on.

Implemented. The Program performed an evaluation of the record types and established procedures requiring periodic reviews of those record types that were determined to be critical.

Implemented. Program management evaluated its systems and determined that only those systems on the mainframe were mission critical. The Program had a disaster recovery plan in place to address mainframe system recovery.

APPENDIX 4

STATUS OF CURRENT AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.1 and B.1	Implemented.	No further action is required.
C.1 and D.1	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

APPENDIX 5

STATUS OF PRIOR AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required	
A.1, A.2, A.3, B.1, B.2, B.3, C.1, E.1, F.1, F.2, G.2, H.1, I.1, J.1, J.2, K.1, L.1, L.2, L.3, and M.1	Implemented.	No further action is required.	
D.1, D.2, and G.1	Resolved; not implemented.	No further response to the Office of Inspector General is required. The information regarding the status of these recommendations will be provided to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.	



U.S. Department of the Interior Office of Inspector General

AUDIT REPORT

GENERAL CONTROLS OVER THE AUTOMATED INFORMATION SYSTEM, ROYALTY MANAGEMENT PROGRAM, MINERALS MANAGEMENT SERVICE

> REPORT NO. 98-I-336 MARCH 1998



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL. Washington, D.C. 20240

MAR 2 A 1998

MEMORANDUM

TO:

The Secretary

FROM:

Robert J. Williams Potent of Williams

Acting Inspector General

SUBJECT SUMMARY: Final Audit Report for Your Information - "General Controls

Over the Automated Information System, Royalty

Management Program, Minerals Management Service" (No.

98-I-336)

Attached for your information is a copy of the subject final audit report. The objective of our audit was to evaluate the adequacy of the general controls over the Minerals Management Service Royalty Management Program's automated information system in the areas of security program development, physical and logical access, software development and change management, separation of duties, system software, and service continuity.

We found that the Royalty Management Program had established general controls over its automated information system; however, except for the controls over physical access to the automated information system, we concluded that the general controls were not adequate in the six major areas reviewed. Specifically, the Program did not identify and address all risks affecting proprietary and financial data in the automated information system, have adequate security-related personnel policies and procedures, and have security awareness statements on file for all employees who used the automated information system; have adequate logical access controls in the areas of resource classification, default settings, commercial off-theshelf software access controls, access levels granted to users, and numbers of allowed log-in attempts: have controls to ensure that client/server application software changes were authorized, approved, and tested before being moved into production; separate the duties of the client/server application programmers from the duties of the users and separate the duties of client/server security administrators from reviewers; use mainframe security software that was supported by the vendor and use available mainframe computer system audit tools to ensure integrity over system processing and data; and include local area networks and personal computers which maintain proprietary and financial data in the Program's disaster recovery plans. We made 24 recommendations to improve the general controls over the Program's automated information system.

Based on the response to the draft report from the Director, Minerals Management Service, we deleted one recommendation and revised one recommendation. Also, based on the response, we considered 1 recommendation resolved and implemented and 12 recommendations unresolved, and we requested additional information for 10 recommendations.

If you have any questions concerning this matter, please contact me at (202) 208-5745.

Attachment



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

MAR 23 1998

AUDIT REPORT

Memorandum

Director, Minerals Management Service To:

Robert J. Williams Robert J. Williams
Acting Inspector General From:

Subject: Audit Report on General Controls Over the Automated Information System,

Royalty Management Program, Minerals Management Service (No. 98-I-336)

INTRODUCTION

This report presents the results of our audit of the general controls over the automated information system at the Minerals Management Service's Royalty Management Program. We performed this audit to support our audit of the Service's financial statements, which is required by the Chief Financial Officers Act. The objective of this audit was to evaluate the adequacy of the general controls over the Program's automated information system in the areas of security program development, physical and logical access, software development and change management, separation of duties, system software, and service continuity.¹

BACKGROUND

The Minerals Management Service's Royalty Management Program is responsible for collecting and disbursing revenues of about \$4 billion annually that are generated from leasing Federal and Indian lands and for collecting royalties for minerals extracted from leased lands. To aid in accomplishing its mission objectives and meeting its financial reporting requirements, the Program uses an automated information system that includes a mainframe computer, a minicomputer, and personal computers and servers which support local area networks for each Program division, a wide area network, and an enterprisewide

¹Logical access refers to controls that provide a technical means of controlling what information users can utilize, the programs they can run, and the modifications they can make. (An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, National Institute of Standards and Technology.)

network.² For collecting rents and royalties, the Program primarily uses the mainframe computer. For disbursing rents and royalties, verifying collections, and reporting financial information, the Program uses all of the components of its automated information system.

The Program's mainframe computer, minicomputer, and some of the personal computers and servers are located in three buildings at the Denver Federal Center, in Denver, Colorado. The Program also has personal computers and servers located in leased buildings in Golden, Colorado, and at Program division offices in Dallas and Houston, Texas.

Since 1992, Program management has been planning, developing, and moving to a "client/server" processing environment.³ In a client/server environment, data are more difficult to protect. Specifically, the data are stored and processed in multiple locations, and the data must travel through telecommunication systems between the clients and the servers where the data are inherently susceptible to being released to unauthorized outside parties, lost, or damaged. Additionally, the Program's data are "proprietary"; therefore, if access to the data is denied or if the data are inappropriately released, lost, or damaged, the Program, suppliers of the data, or others having an interest in the data could be adversely impacted.

The Program's automated information system was operated and maintained by the contractor American Management Systems Operations Corporation. The contract with the Corporation requires the Corporation to: (1) maintain system software; (2) maintain and develop application software; and (3) maintain other software, such as teleprocessing and general utilities.

Overall system security policies for the Program are established by the Installation Automated Information System Security Officer, within the Program's Systems Management Division. System security administration for the mainframe computer, the minicomputer, the wide area network, and the enterprisewide network is the responsibility of the Corporation. Security administration for the Program's local area networks is the responsibility of each of the Program's seven divisions, which consist of the Accounting and Reports Division, the Royalty Valuation Division, the Systems Management Division, the State and Indian Compliance Division, and the Compliance Divisions at Dallas and Houston and Lakewood, Colorado.

²Servers are computers that provide services to client computers on a network. Local area networks are communication networks located in a small geographical area which connect many computerized input/output devices, generally server computers, client computers, and peripheral hardware such as printers, through low-cost communication mediums. These networks typically do not use common carrier circuits, such as U.S. West, and their circuits do not cross public thoroughfares or property owned by others. Wide area networks span large geographical areas and typically use circuits provided by common carriers. Enterprisewide networks are networks that result when all the networks in a single organization are connected together. (Jerry Fitzgerald and Alan Dennis, <u>Business Data Communications and Networking</u>, 5th edition, John Wiley & Sons, Inc., 1996, pps. 249, 522, 529, 542, and 549.)

³A "client/server" processing environment is a computerized architecture in which one or more "computers called servers manage shared resources and provide access to those shared resources as a service to their clients," which are personal computers. (David Vaskevitch, <u>Client /Server Strategies</u>, a <u>Survival Guide for Corporate Reengineering</u>, IDG Books Worldwide, Inc., San Mateo, California, 1993, page 96.)

SCOPE OF AUDIT

To accomplish our objective, we reviewed the general controls that were in place during January through June 1997. Specifically, we reviewed the controls in six major areas: security program development; logical and physical access; software development and change management; separation of duties; system software; and service continuity. We interviewed Program and contractor personnel, reviewed systems documentation, observed and became familiar with computer center operations and network components, analyzed system security, and evaluated service continuity procedures and testing. In addition, we reviewed procedures to maintain system and application software for the mainframe computer, the local area networks, the wide area network, and the enterprisewide network. Because our review was limited to evaluating the adequacy of general controls over the automated information system, we did not evaluate the effectiveness of manual control procedures that may have operated as compensating controls for the automated information system general controls. While our objective was to review the general controls of the automated information system, the primary emphasis was on the servers that supported data processed and maintained on the local area, wide area, and enterprisewide networks.

Our audit, which was conducted during December 1996 through August 1997 at the Program's facilities in Denver and Golden, was made in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we evaluated the internal controls that could adversely affect the Program's automated information system. The control weaknesses that we found are summarized in the Results of Audit section and discussed in detail in Appendix 1 to this report. If implemented, our recommendations should improve the internal controls in the areas reviewed. Because of inherent limitations in any system of internal controls, losses, noncompliance, or misstatements may occur and not be detected. We also caution that projecting our evaluations to future periods is subject to the risk that controls or the degree of compliance with the controls may diminish.

PRIOR AUDIT COVERAGE

During the past 5 years, the General Accounting Office has not issued any reports related to the objective and scope of this audit. However, in July 1997, the Office of Inspector General issued the report "Royalty Management Program's Automated Information Systems, Minerals Management Service" (No. 97-I-1042), which identified weaknesses in mainframe application software development and change management. During our current audit, we noted that Program management had agreed with the seven recommendations made in our prior audit report and that two of the seven recommendations had been implemented. One of the implemented recommendations and three of the recommendations that were resolved but not implemented affected the change request process (change management), which is discussed in the scope of this audit. We further noted that implementation of the three

recommendations was delayed because of the priority of implementing the changes mandated by the Federal Oil and Gas Royalty Simplification and Fairness Act of 1996.

RESULTS OF AUDIT

The Royalty Management Program had established general controls over its automated information system; however, except for the controls over physical access to the automated information system, we concluded that the general controls were not adequate in the six major areas reviewed. Office of Management and Budget Circular A-130, "Management of Federal Information Resources," and National Institute of Standards and Technology publications require Federal agencies to establish and implement computer security and management and internal controls to improve the protection of sensitive information in the computer systems of executive branch agencies.⁴ Additionally, the Congress enacted laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls over the sensitive information is adequate. Further, the Department of the Interior and the Program have issued policies and procedures to implement general controls to protect sensitive data in automated information systems. The controls were not adequate because Program management had not established necessary policies and procedures, had not assigned responsibilities for ensuring that policies and procedures were developed and followed, and had not held officials accountable for noncompliance with the established controls. The lack of adequate controls increased the risk of (1) unauthorized access and modifications to and disclosure of Program data, (2) theft or destruction of Program software and sensitive information, and (3) loss of critical Program systems and functions in the event of a disaster or system failure.

Overall, we identified 13 weaknesses and made 23 recommendations for improving the general controls over the Program's automated information system. A summary of the weaknesses noted in the six major areas is provided in the following paragraphs, and specific details of the weaknesses and our respective recommendations to correct these weaknesses are in Appendix 1.

Security Program Development

We found weaknesses in the automated information system security program. Specifically, Program management did not identify and address all risks affecting proprietary and financial data in the automated information system, did not have adequate security-related personnel policies and procedures, and did not have security awareness statements on file for all employees who used the automated information system. As a result, there was an increased risk that sensitive data may be impaired or compromised by individuals and that data may be inadvertently disclosed or destroyed or erroneously modified. We made seven recommendations to address these weaknesses.

The Computer Security Act defines "sensitive" data as "any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act."

Access Controls

We found weaknesses in logical access controls over the Program's automated information system. These weaknesses were in the areas of resource classification, default settings, commercial off-the-shelf software access controls, access levels granted to users, and numbers of allowed log-in attempts. As a result, there was an increased risk that sensitive data maintained on the automated information system were vulnerable to unauthorized access, manipulation, and disclosure. We made eight recommendations to address these weaknesses.

Software Development and Change Management

We found that the controls over changes to client/server application software were not adequate. Specifically, Program management did not have controls to ensure that client/server application software changes were authorized, approved, and tested before being moved into production. As a result, there was an increased risk that the most critical client/server application software changes were not made and that client/server applications would not perform as intended. We made one recommendation to address this weakness.

Separation of Duties

We found that Program management did not separate the duties of the client/server application programmers from the duties of the users and did not separate the duties of client/server security administrators from reviewers. As a result, there was an increased risk that accidental or intentional actions by programmers could threaten the integrity of the Program's data and disrupt system processing and that inappropriate actions by security administrators would not be detected or detected timely. We made two recommendations to address these weaknesses.

System Software Controls

We found that the controls over system software were not adequate in detecting and determining inappropriate use. Specifically, the security software in use for the mainframe computer was no longer supported by the vendor, and available mainframe computer system audit tools to ensure integrity over system processing and data were not used. As a result, there was an increased risk that programs and data files would not be protected from unauthorized access and that inappropriate mainframe computer system initialization and processing would not be recorded and identified. Additionally, without periodic reviews of the system audit trails, there was an increased risk that processing problems or unauthorized activities may not be detected or detected timely and that the responsible individual or individuals may not be held accountable for the inappropriate action. We made four recommendations to address these weaknesses.

Service Continuity

We found that local area networks and personal computers used by the Program's divisions which maintain proprietary and financial data were not included in the Program's disaster recovery plans. As a result, there was an increased risk that critical systems may not be recovered in the event of a disaster or system failure. We made one recommendation to address this weakness.

Minerals Management Service Response and Office of Inspector General Reply

In the January 21, 1998, response (Appendix 2) from the Director, Minerals Management Service, to our draft report, the Service stated that of the report's 24 recommendations, it "agree[d]" with 11 recommendations, "partially agree[d]" with 2 recommendations, and "disagree[d]" with 11 recommendations. Based on the response, we deleted one recommendation (No. F.3) and revised one recommendation (No. I.1) in the draft report. Also based on the response, we consider 1 recommendation resolved and implemented and 12 recommendations unresolved, and we request additional information for 10 recommendations. The status of each recommendation is in Appendix 3, and the Service's responses to the recommendations and our comments are presented within each finding.

Additional Comments on Audit Report

The Service said that it "disagree[d]" with the overall "implicit conclusion" that the Royalty Management Program's automated information system was not in compliance with Office of Management and Budget Circular A-130 and that it believes that it is in "substantial compliance with the spirit and intent" of the Circular. Further, the Service stated that the audit report "does not actually deal with the overall or general controls" because we did not review redundant and compensating controls. In addition, the Service stated that "recurring management control reviews have addressed such manual controls and generally found they were working effectively or prompted corrective actions to resolve minor control deficiencies." Further, the Service stated that "audits performed under the Chief Financial Officers Act of 1990 have covered these controls, and each report concluded that our financial information was reliable."

The criteria we used included not only Office of Management and Budget Circular A-130 but also standards and guidelines referenced in the Circular from the Department of Commerce (National Institute of Standards and Technology), the General Services Administration, and the Office of Personnel Management and policies and procedures of the Department and the Program. Since the controls cited in and referenced by Appendix III of Circular A-130 are "a minimum set of controls" to be included in an agency's automated information security program, we believe that any deviation from these minimum controls would indicate that an agency's automated information system security program does not reduce risk to an acceptable level and ensure that an agency is in compliance with the Circular. However, since our review identified weaknesses in the general controls over the

automated information system in the areas of security program development, access controls, software development and change management, separation of duties, system software controls, and service continuity, we do not believe that the Service's "substantial compliance" with the minimum controls set forth in the Circular was adequate to address the potential risks identified by our review.

While we stated that we did not evaluate the effectiveness of manual control procedures which may have operated as compensating controls in the scope section of the report, the audit staff did evaluate the general controls that were defined in the Program's policies and procedures. Because redundant or compensating controls were not cited by the Program in its policies and procedures as the primary controls used to ensure the integrity, confidentiality, and availability of Program information, these controls were not evaluated.

During the audit, we reviewed an Automated Information Systems Review that the Service performed in fiscal year 1996 which concentrated on the Program's change management controls over applications in the mainframe environment. The Service's review identified weaknesses concerning application testing and documentation that we also cited in the Prior Audit section of this report. Further, we found similar weaknesses in software development and change management controls in the client/server environment (see Finding I in Appendix 1.)

While we are not questioning that the financial statements were presented fairly, we found, as a result of our evaluation, inadequacies in the Program's general controls over the automated information system in the areas of security program development, access controls, software development and change management, separation of duties, system software controls, and service continuity. These weaknesses, identified with the general controls, will result in our having to raise the overall level of risk of possible loss associated with the internal control structure of the Royalty Management Program in future financial statement audits.

Regarding system security, we agree that system security controls implemented should be measured against costs and risks. However, the Program did not provide evidence that such a measurement study was performed. Further, our findings identified breakdowns in existing controls cited in the Program's policies and procedures. While no system is completely free of errors, an adequate security program would provide a foundation for the Service to determine what controls were operating effectively and the level of risk that the Service is mitigating with these controls.

We disagree that the Program is being held to "unattainable standards" because the standards we used were those cited in Appendix III of Circular A-130 as "the minimum set of controls" to be included in an agency's automated information security program. In addition, in our evaluation of the Program's general controls as defined in its policies and procedures, we found that the controls were not operating effectively.

We disagree with the Service's statement that our findings did not demonstrate a "single negative impact" because the impact of these inadequacies taken as a whole indicates that there is no assurance that the overall risk to the Program was at an acceptable level.

In accordance with the Departmental Manual (360 DM 5.3), we are requesting a written response to this report by April 17, 1998. The response should provide the information requested in Appendix 3.

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued, actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Minerals Management Service personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

SECURITY PROGRAM

A. Risk Assessments

Condition: Risk assessments of the Royalty Management Program's automated information system did not identify and address all risks affecting proprietary and financial data in the automated information system or correctly assess some of the risk elements. For example, we found that Program management did not:

- Identify and address the impact that (1) converting to the year 2000 would have on application processing, (2) using system security software which is no longer supported by the vendor could have on operations, and (3) having royalty and financial information on local area network applications and personal computer databases could have on operations.
- Correctly assess the risk for the "Geopolitical" and "External Directives" elements, which were assessed as low risk. Significant geopolitical and external directives, such as the possible abolishment of the Program and the enactment of the Federal Oil and Gas Royalty Simplification and Fairness Act, have impacted the Program during the past 2 years. We believe that the level of risk associated with these elements was such that it increased the potential for lowering employee morale and thus increased the risk of sabotage or breach of other physical security measures, as well as the possibility of data errors and omissions that affect data and system integrity.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," states that adequate security "includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls." The Circular further states that, although formal risk analyses need not be performed, "the need to determine adequate security will require that a risk-based approach be used." According to the Circular, "This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards." Also, the National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" provides guidance on computer security risk management. The NIST Handbook specifically addresses the

selection of safeguards to mitigate risk and the acceptance of residual risk. In addition, Program policy requires that local area network administrators participate in the risk assessment process.

Cause:

Program management did not ensure that risk assessments were performed in accordance with risk management guidelines. Specifically, the assessments did not address (1) all risks associated with its automated information system, (2) the selection of safeguards to mitigate risks, and (3) the acceptance of residual risk. In addition, Program management did not effectively communicate the responsibility of local area network administrators to participate in risk assessments and had not adequately addressed that local area network applications and personal computer databases should be included in the Program's security program.

Effect:

Without identifying all significant threats and vulnerabilities to the automated information system, Program management was unable to determine the most appropriate measures needed to protect against threats or reduce the vulnerabilities. Further, without including the Program's local area network applications and personal computer databases as part of the risk assessments, there was little assurance that all threats and vulnerabilities were identified and considered when Program security policies and plans were developed. Therefore, there was an increased risk that critical Program resources would not be adequately protected and that expensive controls would be implemented for resources that did not require significant protection.

Recommendations:

We recommend that the Director, Minerals Management Service:

- 1. Ensure that risk assessments are conducted in accordance with guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the assessments should address significant risks affecting systems, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of the residual risk.
- 2. Formally assign and communicate responsibility to local area network administrators to participate in risk assessments and ensure compliance with the Program's security policy.
- 3. Determine the risks associated with local area network applications and personal computer databases which contain proprietary and financial data and, based on the results of the risk assessments, establish appropriate security policies and procedures.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service provide additional information for Recommendation 3 and that it reconsider its responses to Recommendations 1 and 2, which are unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service stated that it "plans to enhance and better document" its risk assessment process. The Service further stated that it believed its "previous assessments were in accordance with guidelines" because of the "rapidly changing computing and communication environment."

Office of Inspector General Reply. We disagree that "previous assessments were in accordance with guidelines." Office of Management and Budget Circular A-130, Appendix III, and referenced standards and guidelines of the National Institute of Standards and Technology state that "risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk." Since the Service did not address a number of significant conditions/issues that affect risks to the Program's automated information system, identify the risks associated with these conditions, or identify the controls in place to reduce the risks to an acceptable level, we believe that the Program's risk assessment process was not in accordance with the guidelines. Additionally, Appendix III of Circular A-130 was revised so that Federal computer security programs could better respond to the rapidly changing technological environment. Although the Service disagreed with the recommendation, we believe that its action to enhance and document its risk assessment process is indicative of its intent to comply with the recommendation. However, we request that the Service clarify its intent (see Appendix 3).

Recommendation 2. Nonconcurrence.

Service Response. The Service stated that policies "define the LAN [local area network] administrators' role in contingency planning and security," and it provided additional information to support its position.

Office of Inspector General Reply. While the additional information did address the administrators' role in contingency planning and security, it did not address the recommendation. The "RMP Automated Information Systems Security Manual" states that administrators should participate in the risk assessment process. During our audit, we found

that the administrators were not always aware of their responsibilities to identify risks and implement controls that would mitigate risks and that the administrators' individual position descriptions did not always address these responsibilities.

Additional Comments on Finding

The Service stated that it believes that we did not apply risk assessment criteria appropriately because "Circular A-130 states 'the Appendix no longer requires the preparation of formal risk analyses' and that risk assessments 'can be formal or informal, detailed or simplified, high or low level, quantitative (computationally based) or qualitative (based on descriptions or rankings), or a combination of these. No single method is best for all users and all environments."

We agree that formal risk analyses are not required and that risk assessments can be formal or informal. However, we found that the Program's analyses were not based on risk-based management as described by Appendix III of Circular A-130 and referenced standards and guidelines of other Federal executive branch agencies and the Departmental Manual (375 DM 19). According to the NIST Handbook, risk-based management "is the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk." In its response, the Service provided additional information related to each of the examples in this finding. However, the additional information provided did not indicate that the Program used risk-based management in developing its controls.

B. Security-Related Personnel Policies and Procedures

Condition: The Program's security-related personnel policies and procedures were not adequate to ensure system integrity. Specifically, we found that:

- Contractor employees received the same type of background check and security clearance regardless of their duties and the risk associated with the computer-related work they performed. Thus, contractor employees, such as system programmers and computer operators, who could bypass technical and operational controls, received the same security clearance as administrative assistants.
- Computer-related work was not technically reviewed by contractor or Program personnel whose position sensitivity was greater than that of the position sensitivity of individuals performing the work.
- Contractor employees did not always submit requests for background checks for security clearances. Further, the requests that were submitted for background checks were not submitted within the time frames specified in the contract. An average of 175 calendar days elapsed, instead of the 2 weeks stipulated in the contract, between the dates the employees were hired and the dates the requests were received by the Minerals Management Service's Security Officer in Personnel for forwarding to the Office of Personnel Management. The Office of Personnel Management performed background checks for the same employees in an average of 84 days, and the Minerals Management Service approved the security clearances in an average of 22 days. Thus, most of the delay in the security clearance process was attributable to contractor and Program personnel.
- Systems Management Division employees did not have documentation to support that appropriate background checks for security clearances and required periodic followup background checks had been performed.

Criteria:

The Departmental Manual (441 DM) specifies that position sensitivity should be based upon risk factors such as degree of public trust, fiduciary responsibilities, importance to program, program authority level, and supervision received. In addition, the Manual requires consideration of automated data processing (ADP) factors, such as the level of responsibility and technical review of work, for incumbents who are responsible for planning, directing, and implementing computer security; planning, directing, implementing, operating, and maintaining computer systems; and accessing or

processing automated information records systems that contain proprietary data. Further, work is to be technically reviewed by individuals filling ADP "critical-sensitive" positions when individuals filling ADP "noncritical-sensitive" positions perform computer work such as directing, planning, designing, operating, and maintaining a computer system to ensure system integrity. In addition, the terms of the contract require that the "assistant manager" positions' sensitivity level be ADP "critical-sensitive," that background check requests be submitted to the Service within 2 weeks after an employee's hire date, and that the employees be in probationary status until the background checks are completed and the security clearances are approved.

Cause:

The Systems Management Division staff and the contractor staff who were responsible for technical reviews of the work were not in positions classified as ADP "critical-sensitive." Additionally, Program contracting personnel did not ensure that contractor personnel (1) submitted requests for background checks and (2) remained in probationary status and did not perform critical computer work until background checks were completed and security clearances were approved. Further, personnel or security files did not reflect that appropriate background checks or that required periodic followup background checks were performed.

Effect:

As a result, there was an increased risk that employees would perform critical automated information system operations and maintenance work without appropriate oversight or adequate assurance that their backgrounds would warrant such trust.

Recommendations:

We recommend that the Director, Minerals Management Service:

- Evaluate Systems Management Division and contractor ADP positions to determine
 position sensitivity in relation to risk and ADP factors. Also, assurance should be provided
 that automated information system work is technically reviewed by persons whose position
 sensitivity levels are greater than the position sensitivity levels of the employees who are
 performing the work.
 - 2. Establish controls to ensure that the contractor is fulfilling its contractual obligation of submitting requests for background checks within the specified time frame and that contractor employees who are in probationary status and awaiting security clearances are not performing critical ADP work.

3. Establish controls to ensure that personnel or security files accurately reflect that background checks and periodic followup background checks are performed as required.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service provide additional information for Recommendations 1 and 2 and that it reconsider its response to Recommendation 3, which is unresolved (see Appendix 3).

Recommendation 1. Partially concur.

Service Response. The Service stated it planned to "reevaluate the position sensitivity level for the senior personnel in charge of the contractor activity to determine if those position[s] should be classified at a higher level. In accordance with Departmental criteria, most ADP [automated data processing] staff are designated noncritical sensitive. We doubt it was the OIG's [Office of Inspector General] intention to imply that *all* work must be reviewed by persons at a higher sensitivity level; however, this would be impossible in a multiple level organization because there are only two sensitivity levels from which to choose, i.e., 'noncritical-sensitive' and critical-sensitive.'"

Office of Inspector General Reply. The Departmental Manual identifies four sensitivity levels. Further, although the Service indicated that some staff would have the next higher security level of "critical-sensitive" to perform technical reviews, we found that only one ADP staff position was classified as "critical-sensitive" and that the position was not responsible for performing technical reviews. Although the Service only partially concurred with the recommendation, we believe that the action to reevaluate position sensitivity levels is indicative of its intent to comply with the recommendation.

Recommendation 2. Partially concur.

Service Response. The Service said that it agreed that controls were needed to ensure that the contractor submitted requests for background checks in a timely manner. The Service further stated that the contractor had been "directed" and had "begun to track and is accountable for the status of its submission of these requests." The Service also said that it agreed that contractor employees awaiting clearances should be in "probationary status" but that having the employees not performing their assigned duties would be "unacceptably costly." According to the Service, it was "exploring alternatives" with the contractor such as having the contractor "perform a preliminary 'criminal and credit check' which is quick and inexpensive."

Office of Inspector General Reply. Preliminary investigations would be a suitable alternative to prohibiting contractor employees from performing their assigned duties before the background clearances have been accomplished. Although the Service only partially concurred with the recommendation, we believe that its action to evaluate alternatives such as preliminary investigations is indicative of its intent to comply with this recommendation.

Recommendation 3. Nonconcurrence.

Service Response. The Service stated that controls are "in place to ensure that personnel or security files accurately reflect background checks." The Service further stated that its Office of Administration and Budget "maintains documentation and a tracking system" on all security clearances and background checks of its employees and contractors. The Service stated that it disagreed with our statement that followup background checks are required, stating that it is in compliance with Department of the Interior guidance which states that followup checks "are authorized *only* for national security positions and not for public trust positions."

Office of Inspector General Reply. The Office of Administration and Budget's documentation and tracking system, while serving as part of the control, did not ensure that personnel or security files accurately reflected that background checks were requested and documented in the "official personnel files" of the employees. Additionally, the Departmental guidance included by the Service was dated 1993; however, the Code of Federal Regulations (5 CFR 1), dated 1997, states that followup background checks are required of employees in positions that are for national security and other positions considered to be "high risk." The Office's Security Officer verified that the Program has employees in "high risk" positions, such as the Chief, Systems Management Division; the Installation Security Officer; the Contractor's Project Manager; and supervisors within the Systems Management Division. As such, employees in these positions would be required to have followup background checks.

SECURITY PROGRAM

C. Security Awareness Statements

Condition: We found that automated information system users did not have security

awareness statements on file acknowledging the employees' acceptance of their

responsibilities to safeguard the Program's proprietary data and assets.

Criteria: The Department's "Automated Information Systems Security Handbook"

requires employees who use sensitive automated information system resources to sign statements acknowledging their responsibilities for the security of the resources. Additionally, the "RMP [Royalty Management Program] Automated Information Systems Security Manual" requires that employees sign a Minerals Management Service Security Statement, which acknowledges their responsibilities to safeguard Program-sensitive data and assets, and requires the Installation Automated Information System Security Officer (Installation Security Officer) to verify that security awareness statements are signed by the

employees before their system access requests are approved.

Cause: Program management did not ensure that its employees signed security

awareness statements. In addition, the Installation Security Officer did not ensure that security statements were on file before the Installation Security

Officer approved access to the automated information system.

Effect: As a result, employees may not be aware of their responsibilities to safeguard

automated information system data and assets and thus inadvertently disclose

sensitive information.

Recommendation:

We recommend that the Director, Minerals Management Service, establish controls to enforce Program policy which requires employees to sign security awareness statements before access to system resources is approved by the Installation Automated Information System Security Officer.

SECURITY PROGRAM

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service reconsider its response to the recommendation, which is unresolved (see Appendix 3).

The Service stated that while its own test sample confirmed that users have appropriate access to the Program's systems, it "concur[s] that [its] filing system for access approvals needed improvement." The Service further stated that all statements are "now consistently filed and reconciled by the ADP security officer."

The Service agreed with the recommendation and said that it was implemented. However, while the security awareness statements referred to in the finding provide evidence that users accepted their responsibility to safeguard the Program's proprietary data and assets, these statements do not support the appropriateness of access to Program systems. Without familiarity with the methodology employed in the Service's test, such as sample selection and test performance, we must rely on the tests performed using statistical sampling software and generally accepted Government auditing standards followed by the audit staff. Further, the Service stated, in its response to Recommendation D.2, that "all MMS [Minerals Management Service] employees are granted access to view royalty, production, and reference data." Accordingly, if the Service's tests did not include all Service employees, there is no assurance that all statements have been filed and reconciled. Therefore, we consider this recommendation unresolved and request that the Service reconsider its response to the recommendation (see Appendix 3).

D. Resource Classifications

Condition: The Program's computer resources (data files, application programs, and computer-related facilities and equipment) were not classified appropriately to determine the levels of access controls that should be implemented over the resources. For example, no "major application" was identified in the Program's annual security plan, even though the applications and data files were "proprietary" and critical to the Program in accomplishing its mission and reporting financial information. Further, access controls over sensitive data on the servers used by the Program's divisions were not as stringent as the access controls over sensitive data on the mainframe.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, directs agencies to assume that all major systems contain some sensitive information that needs to be protected but to focus extra security controls on a limited number of particularly high-risk or major applications. According to the NIST Handbook, "Security levels, costs, measures, practices, and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability, and extent of potential harm." Further, the determinations should flow directly from the results of risk assessments that identify threats, vulnerabilities, and the potential negative effects that could result from disclosing confidential data or failing to protect the integrity of data supporting critical transactions or decisions. Accordingly, Program policy requires that users be given access only to the resources needed to perform their assigned duties.

Cause:

Program management had not identified the resources that needed significant protection. Further, Program management did not require application owners who are responsible for approving user access levels to the applications to classify their resources based on the level of sensitivity of the information contained in their applications.

Effect:

As a result, there was an increased risk that resources were not adequately protected from unauthorized access and disclosure and therefore were subject to either accidental or intentional changes to computer operations and data.

¹Office of Management and Budget Circular A-130, Appendix III, identifies a "major application" as an "application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application." The Appendix further states that "certain applications, because of the information in them, however, require special management oversight and should be treated as major."

Conversely, the level of protection provided for low-risk resources may be in excess of that required. Furthermore, Program management did not have a reliable basis for making critical decisions regarding security safeguards for its sensitive applications.

Recommendations:

We recommend that the Director, Minerals Management Service:

- 1. Ensure that individual computer resources are classified based on the level of sensitivity associated with each resource.
- 2. Evaluate controls over resources to ensure that the access controls have been implemented commensurate with the level of risk and sensitivity associated with each resource.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service reconsider its response to Recommendations 1 and 2, which are unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service said that it believed that its "current classifications are appropriate." The Service further stated that its mainframe systems "receive heightened security because they are more mission critical, not because they are more sensitive" and that these systems "must be protected more strenuously to ensure the integrity of the official records." The Service also stated: "A more moderate level of protection is necessary for proprietary information than for mission critical information. The umbrella protection mechanism for all types of proprietary information is physical controls coupled with employee training."

Office of Inspector General Reply. We disagree that the Service's current classifications are appropriate. In its response to Recommendation M.1, the Service indicated that the Program had not identified all "mission critical" systems. Further, in our opinion, mission critical systems resided on personal computers and local area networks that supported the Program's mission to accurately and timely disburse rents, bonuses, and royalty revenues to the U.S. Treasury, the states, and the Indian tribes, as well as financial transactions and external reporting. Additionally, the Service stated that the umbrella protection over its proprietary data, which do not reside on the mainframe computer, is

limited to "physical controls" and "employee training." However, these controls do not meet the minimum controls required for Federal automated information resources. The purpose of resource classification is to provide a basis for determining the controls necessary to ensure appropriate implementation of risk-based management, as required by Office of Management and Budget Circular A-130, Appendix III.

Recommendation 2. Nonconcurrence.

Service Response. The Service said that it believes that its "existing access controls over resources already meet the intent of this recommendation." The Service further stated that all of its employees "are granted access to view royalty, production, and reference data. Since most of this data is proprietary, employees are trained in its proper use and must sign statements acknowledging their responsibility to protect it. State and Tribal employees have access to such data within their jurisdictions only. The ability to add or change data is limited to those employees who require that access to perform their jobs."

Office of Inspector General Reply. We disagree that the Service's existing access controls meet the intent of the recommendation. By its response, we inferred that the Service had not complied with the personnel control of "least privilege" required by Appendix III of Circular A-130 and the "RMP Automated Information Systems Security Manual." The Circular defines least privilege as "the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read [which means to view], write, execute, delete) to the minimum necessary to perform" an employee's job. Further, the Program's Manual states, "[P]rivileges granted to users are only those privileges that are absolutely necessary for job performance." In addition, Appendix III of Circular A-130 and the Departmental Manual (375 DM 19) state that the "greatest threat" to most computer systems comes from authorized users. However, as stated by the Service, "All [Service] employees are granted access to view royalty, production, and reference data." Therefore, we believe that allowing all Service employees to have access to view Program data indicates that access controls were not implemented commensurate with the level of risk and sensitivity of each resource. Further, as cited in Findings E, F, and G in this report, controls over access were inadequate; therefore, we believe that the Service's current access controls over resources do not meet the intent of the recommendation.

E. Default Settings Provided With Commercial Off-the-Shelf Software

Condition: Default settings provided with commercial off-the-shelf software were not

removed after the software was installed and implemented. For example, we found that the default user identification (ID) and associated default password had not been removed when Program management upgraded to the latest version of the Integrated Data Management System (IDMS).² The default user ID provides users with administrative privileges to establish and remove users

and to access all mainframe computer resources.

Criteria: The "RMP Automated Information Systems Security Manual" requires that

default user IDs and passwords be removed once commercial off-the-shelf

software is implemented.

Cause: Rather than deleting the default user ID and password, Program management

relied on the mainframe security software to protect against unauthorized

access.

Effect: As a result, there was an increased risk that the automated information system

could be accessed by unauthorized users.

Recommendation:

We recommend that the Director, Minerals Management Service, implement controls to enforce Program policy that default user IDs and passwords are to be removed from the automated information system when commercial off-the-shelf software is implemented.

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service indicated agreement with the recommendation. However, the Service needs to provide additional information for the recommendation (see Appendix 3).

Additional Comments on Finding

Even though the Service agreed with this recommendation, it stated that our conclusion was incorrect that "the use of this default ID allows access to all mainframe computer resources" because "the security architecture prevented" the misuse of resources. The security

²Integrated Data Management System (IDMS) is a licensed product of Computer Associates International, Inc., which manages database applications that reside on mainframe computers.

architecture requires that a user who wants to access the mainframe have a "valid RACF logon password" and a "user ID defined to the data dictionary." We disagree that the security architecture prevented the misuse of resources. Vendor documentation states that the default ID can be used to establish a user in the dictionary and perform all activities cited in this finding. In addition, we found that at least two applications did not rely on the Program's "security architecture."

F. Commercial Off-the-Shelf Software Access Controls

Condition: Commercial off-the-shelf software access controls were not implemented to safeguard against unauthorized access to the mainframe computer, personal computers, and servers. Specifically, we found that:

- Resource Access Control Facility (RACF)³ provides the capability to set rules for passwords in which the installation can require the use of specific characters (a mix of letters and numbers) within the passwords, but this feature was not used.
- A default security setting was found on a server file that allows passwords to be unencrypted.
- The "SECURE CONSOLE" command was not found on a server file which removes the Disk Operating System (DOS) from the server memory. The removal of DOS from the server memory prevents an individual from inserting a diskette into the server drive and loading unauthorized software that could perform such functions as change passwords, establish trustee rights, create users, and assign security levels. Also, the "SECURE CONSOLE" command disables the users' ability to change the server date and time, thus allowing users to bypass access restrictions.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Also, the Department's "Automated Information Systems Security Handbook" states that proprietary, personnel, sensitive, and mission-critical information should be protected from unauthorized disclosure. In addition, the Program's Automated Information Systems Security Manual states that a mix of letters and numbers is recommended for passwords used to access the Program's automated information system.

Cause:

The Program's policy recommended rather than required the use of a mix of both letters and numbers in passwords to access its automated information

Resource Access Control Facility (RACF) is an IBM-licensed software security product that protects information by controlling access to the information. RACF provides security by identifying and verifying users to the system, authorizing users' access to protected resources, and recording and reporting access attempts. (Resource Access Control Facility General Users Guide, Version 1. Release 9.2, 9th edition, IBM Corp., 1993, page 1-1.)

system. In addition, there was no centralized security administration for the local area networks and personal computers that contain proprietary and financial data, and no Program procedures were in place to ensure that controls were adequate to safeguard these local area networks and personal computers.

Effect:

As a result, there was an increased risk that unauthorized access could be gained to the automated information system, which could result in the loss of data and in unauthorized individuals gaining access to sensitive data files.

Recommendations:

We recommend that the Director, Minerals Management Service:

- 1. Evaluate the current Program policy which only recommends that passwords contain a mix of letters and numbers for all automated information system components. Implement, if the Program determines that a mix of letters and numbers should be required, the security software option within RACF that would enforce this requirement. If the Program determines that a mix of letters and numbers is not required, the risk should be addressed in the risk assessment.
- 2. Develop and implement centralized security administration for the local area networks used by the Program's divisions that contain proprietary and financial data.

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service indicated agreement with both recommendations. However, the Service needs to provide additional information for Recommendations 1 and 2 (see Appendix 3).

G. Access Levels Granted

Condition: We found that controls were not adequate to ensure that access levels granted to users of the Program's automated information system were appropriate. Specifically, access managers had not approved all automated information system access granted to users of the access managers' applications and had not performed periodic reviews to determine who the users were and whether the levels of access granted in the automated information system were the access levels approved.

Criteria:

The "RMP Automated Information Systems Security Manual" states that supervisors and managers are responsible for ensuring that employees' ADP access certifications are appropriate for the job they will perform before users are set up to access the automated information system. Also, the "Generally Accepted Principles and Practices for Securing Information Technology Systems," issued by the National Institute of Standards and Technology, states: "It is necessary to periodically review user account management on a system." Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, [and] whether management authorizations are up-to-date."

Cause:

Program management had not ensured that its policies were implemented effectively because access managers were not included in the process of approving access to the automated information system. Additionally, the Program's policies and procedures did not require that access managers perform periodic reviews of users' levels of access to application files and system records. In addition, Program management could not efficiently, through automated means, perform reconciliations of authorization forms and access levels granted in the automated information system because the audit tools available for the automated information system had not been acquired. Although automated capabilities were not acquired, Program management could ensure that user access levels were appropriate to the work performed through a recertification process whereby users resubmit the ADP access certifications annually.

Effect:

As a result, there was an increased risk that unauthorized access, data manipulation, or disclosure of proprietary information may occur. In addition. a periodic review of access files may limit the damage resulting from accidents, errors, or unauthorized use of automated information system resources and increase assurance that access levels were revised when users were reassigned or promoted or they terminated their employment. Additionally, since periodic

reviews were not performed, there was an increased risk that unauthorized access would not be detected or detected timely.

Recommendations:

We recommend that the Director, Minerals Management Service:

- 1. Implement controls to ensure that access managers approve all access to their applications in accordance with Program policy.
- 2. Document procedures which require that users' access levels be reviewed periodically or that employees be recertified to ensure that the levels of access granted are appropriate for the duties assigned to the users.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service reconsider its responses to Recommendations 1 and 2, which are unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service stated that it believes that "effective controls have been in place to assure that application managers approve all access to their applications." It further stated that it "acknowledge[d] that our filing system for such approvals needed improvement and are in the process of resolving this problem."

Office of Inspector General Reply. We disagree that effective controls were in place which ensured that application managers approved all access to their applications. We found that the Program did not enforce its policy which required application managers to approve all access granted to users of their applications. We performed a statistical test of users who had access to Program applications and production data and found that over 10 percent of those users tested did not have their access approved by the application manager or the Installation Security Officer. We discussed access approvals with application managers and found that these managers were unaware of how many of the users had access to the managers' applications. Therefore, the problem was not attributable to the "filing system" but to the lack of enforcement of Program policy.

Recommendation 2. Concurrence.

Service Response. The Service stated that it "concur[red] with the need to document these procedures" but "disagree[d] with the OIG's [Office of Inspector General] implication (in its statement of effect) of any significant risk of security breaches." The Service further stated: "Access to mission-critical systems has been carefully managed and controlled through documented security procedures and controls, including mainframe access matrices and annual reviews by the Security Manager. Our own tests confirmed that no unauthorized access exists or has existed."

Office of Inspector General Reply. The Service agreed that procedures should be documented but stated that it had procedures and controls in place for mission-critical systems. However, we disagree that adequate procedures and controls were in place because the Program's procedures did not address periodic reviews of users' access levels. The Service disagreed that any significant risk of security breaches would occur because mission critical systems are "carefully managed and controlled" through "documented security procedures and controls." Since the Service stated in its response to Recommendation M.1 that it had not identified all mission critical systems, it is unclear how the Service managed and controlled its mission critical systems. Regarding the annual review, under the current version of the security software, a review of user access levels within the system could not be performed. Therefore, the Program's procedures did not ensure that all users' access levels were reviewed periodically and that the levels of access granted were appropriate for the duties assigned to the users, thus ensuring implementation of "least privilege." Further, the use of the matrix identified users within a group and the group's levels of access, but it did not identify access levels for each user. In addition, without familiarity with the methodology employed in the Service's test, such as the sample selection and test performance, we must rely on the tests performed using statistical sampling software and generally accepted Government auditing standards followed by the audit staff.

H. Number of Log-in Attempts

Condition: The Program's number of unsuccessful log-in attempts to access its automated

information system exceeded the standard established by the Department. Specifically, in 1992, Program management increased the number of unsuccessful log-in attempts from three to five before a user's ID and password

were revoked.

Criteria: The Department's "Automated Information Systems Security Handbook" states

that the number of unsuccessful log-in attempts should be three.

Cause: Program management did not follow the Departmental standard because, they

stated, it was difficult for some state and tribal organizations, which are

external customers, to access the mainframe computer through telephone lines.

Effect: As a result, the increased number of invalid attempts reduced the effectiveness

of the password as an access control. Thus, there was an increased risk of

unauthorized access to sensitive information.

Recommendation:

We recommend that the Director, Minerals Management Service, evaluate the need to deviate from the Departmental standard for the number of unsuccessful log-in attempts. If the Program determines that this number should remain at five, Program management should request, from the Department, a waiver from the standard of three attempts.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we consider this recommendation resolved and implemented (see Appendix 3).

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

I. Client/Server Application Software Changes

Condition: Change management controls over client/server application software were not

adequate. Specifically, we found that there were no controls to ensure that: (1) Program management authorized and approved software changes and (2) the changes to the application software were adequately tested before the

changed software was moved into production.

Criteria: National Institute of Standards and Technology Special Publication 500-161,

"Software Configuration Management: An Overview," states that software configuration control management procedures should define the specific steps taken to analyze and evaluate the change request, clarify the meaning of the request, and resolve the problem described. In addition, the procedures should identify the appropriate individuals or organization responsible for evaluating the requests and discuss the submission of the evaluation results to the appropriate review board or individuals for approval or disapproval. Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," states that testing is a critical component of software maintenance and that, as such, test procedures must be consistent and based on sound principles. Further, the Publication states that tests should examine

whether the application software is "doing what it is supposed to do."

Cause: Program management did not enforce procedures for authorizing, approving,

and testing client/server application software.

Effect: As a result, there was an increased risk that the most critical client/server

application software changes were not made and that applications would not

perform as intended.

Recommendation:

We recommend that the Director, Minerals Management Service, enforce its procedures for authorizing, approving, and testing client server application software before the software is moved into production.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service stated that the documented procedures "are already in place."

Although the Service provided additional information in its response showing that client/server software development and change management procedures had been in place since 1995, the information, which we requested, was not provided during our audit. Based on the subsequent information provided by the Service, we agree that the Service has documented procedures. However, we found that these procedures had not been enforced during fiscal year 1997. Specifically, in our review of four client/server applications, we found no evidence to support that software changes were authorized, approved, and tested. Therefore, we have revised this finding and recommendation and request that the Service respond to the revised recommendation (see Appendix 3).

SEPARATION OF DUTIES

J. Duties Related to Client/Server Applications

Condition: The duties related to client/server applications were not separated effectively. Specifically, we found that:

- Application programmers were authorized to access client/server production data to perform "ongoing maintenance" on applications.
- At least one application programmer acted as a backup to an end user, which required the programmer to change production data in the Minerals Management Service Appeals Tracking System.
- The individual responsible for setting up users of the Royalty Management Program Desktop applications was also the person designated to review server security logs, which record the activities of the users of the applications.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires that security controls for personnel include least privilege and separation of duties. The Circular states, "Least privilege is a practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job." Separation of duties is the practice of dividing the steps in a critical function among different individuals. Also, the NIST Handbook states, "Separation of duties refers to dividing roles and responsibilities so that a single individual cannot subvert a critical process." The "RMP Automated Information Systems Security Manual" states, "Access to sensitive data is limited to those persons who use or process the data in performing their official duties."

Cause:

Program management did not appropriately assign duties for application programmers to ensure that critical processes were not subverted. Specifically, programmers should not have access to production data because access to production data should be restricted to users. Also, Program management had not ensured that independent reviews of server security logs were performed periodically.

Effect:

As a result, there was an increased risk that accidental or intentional unauthorized actions by programmers could threaten the integrity of the Program's data and disrupt system processing. Furthermore, there was an

SEPARATION OF DUTIES

increased risk that inappropriate actions by the individuals who established system users would not be detected or would not be detected timely.

Recommendations:

We recommend that the Director, Minerals Management Service:

- 1. Implement controls to ensure that application programmers do not have access to the production client/server application data or the capability to update/change these data.
- 2. Improve detection controls by ensuring that management or the Installation Security Officer reviews server security logs periodically.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service provide additional information for Recommendation 2 and that it reconsider its response to Recommendation 1, which is unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service stated: "While application programmers do not routinely require update access to any RMP [Royalty Management Program] production data, there are instances when temporary access is needed by specific programmers under controlled circumstances. To mitigate any future risks associated with this access, procedures have been reinforced which detail actions to be taken when requesting temporary access to mainframe and client/server production data." The Service also "refute[d]" our statement that application programmers serve as backups to end users.

Office of Inspector General Reply. The Service indicated that procedures were in place to control the risk when application programmers had update access to Program data. However, we did not find such procedures; therefore, we could not test the procedures to ensure that temporary access was provided to specific programmers under controlled circumstances. To resolve this recommendation, the Service is requested to provide documentation of the procedures the Program uses that mitigate risk when programmers are allowed update access to production data.

SEPARATION OF DUTIES

Regarding application programmers serving as backups to end users, we found during our audit that a programmer analyst had been given access to a client/server application to change the database, to make table updates, and to print reports. According to Program personnel who were responsible for the application, this access was authorized so that the programmer could provide backup duties to a Program employee.

Recommendation 2. Concurrence.

Service Response. The Service stated that the contractor was "being directed to address the review of server security logs within their overall internal control procedures."

Office of Inspector General Reply. We accept the Service's alternative of having the contractor review the logs rather than Program management or the Installation Security Officer. However, regardless of who does the review, the procedures must ensure adequate separation of duties between the key functions of the security log reviewer and the security administrator.

K. Security Software

Condition: The version of RACF, the commercial mainframe security software, that was

used by the Program was no longer supported by the vendor. Although the upgraded version of RACF had been purchased, it had not been implemented.

Criteria: Federal Information Processing Standards Publication 106, "Guideline on

Software Maintenance," states that "the goal of software maintenance

management is to keep systems functioning."

Cause: Program management had not implemented the upgraded version of RACF

because management was in the process of requesting a waiver from the Department from consolidating its mainframe operations with another mainframe operation, which has the upgraded RACF, as required by Office of Management and Budget Bulletin 96-02, "Consolidation of Agency Data Centers." If the waiver is granted to the Program, the upgraded version of

RACF will need to be implemented immediately.

Effect: Using security software that was not supported by the vendor increased the risk

that security software would not be maintained and that programs and data files

would not be protected from unauthorized access.

Recommendation:

We recommend that the Director, Minerals Management Service, ensure that the upgraded version of RACF is implemented immediately if the Program is granted a waiver from consolidating its mainframe operations with another mainframe operation.

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service stated that it believes that we "misunderstood the effects of delaying this software upgrade. Although this is a moot point now that MMS [Minerals Management Service] has replaced its processor, the decision not to upgrade the RACF software was well founded."

Although the Service indicated that it had replaced its processor, we were not provided information to determine whether the Service has ensured that the upgraded version of RACF or equivalent security software was implemented on the new processor. Therefore, we

consider this recommendation unresolved and request that the Service reconsider its response to the recommendation (see Appendix 3).

Additional Comments on Finding

The Service stated that the Program "initially delayed the upgrade because it was considering a processor replacement that would require an entire new suite of mainframe software products." The Service further stated, "Upgrading RACF at that time would have been an inherently risky and potentially expensive decision." Regarding these statements, we were not provided any documentation to support these statements that the decision to not implement the upgraded version of RACF was based on the Service's plan to implement a new processor or that the upgrade of RACF would be "risky and potentially expensive."

L. Mainframe Computer System Audit Tools

Condition: Program management did not use available system audit tools to ensure integrity over system processing and data and to detect inappropriate actions by authorized users. Specifically, we found that:

- System integrity verification and audit software was not used. This software could assist data center and installation security management in identifying and controlling the mainframe computer operating system's security exposures such as setting system options inappropriately, installing "back doors" to the operating system, and introducing viruses and Trojan horses, that can destroy production dependability and circumvent existing security measures.
- Computer operators and system programmers had the capability to change the system initialization process and thus affect system processing. Additionally, system options that produce a system audit trail were not implemented. Therefore, an audit trail that logs the results of actions taken by computer operators and system programmers in the SYSLOG during system initialization could not be produced for periodic review.
- Periodic reviews of System Management Facility (SMF) logs to identify critical events affecting system processing were not performed. For example, reviews were not performed of record type 7, which records when the system audit trail is lost, and record type 90, which records events such as "SET TIME," "SET DATE," and "SET SMF," all of which affect system processing and production of audit trails.
- Periodic reviews of SMF logs to identify unauthorized changes to data by authorized users were not performed. Even though one of the SMF record types, record type 60, which logs all activity affecting Virtual Storage Access Method data sets that contain lease and site security data, was activated during our audit, the logs were not reviewed to detect inappropriate actions or unusual activity by authorized users.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In

⁴The System Management Facility (SMF) logs record all system activity and serve as an audit trail of system activity, including identification of users who performed the activity.

addition, the Circular states that individual accountability is one of the personnel controls required in a general support system. The Circular further states that an example of one of the controls to ensure individual accountability is reviewing or looking at patterns of users' behavior, which requires reviews of the audit trails. The NIST Handbook states that audit trails are a technical mechanism to achieve individual accountability.

Cause:

Program management did not acquire system integrity and verification software, did not implement system options to record actions taken affecting system initialization, did not encourage the use of available system audit trails to detect and identify inappropriate actions affecting the system processing and data integrity, and did not establish procedures requiring periodic reviews of resultant logs because the logs were extensive and difficult to read. Further, Program management had not considered converting the logs to a more useful format to extract critical information. Instead, Program management relied on its staff to make appropriate changes to the system initialization process and on authorized users to make only appropriate changes.

Effect:

As a result, inappropriate mainframe computer system initialization and processing were not recorded and identified. Additionally, without periodic reviews of the system audit trails, there was an increased risk that processing problems or unauthorized activities would not be detected or would not be detected timely and that the individual responsible would not be held accountable for the inappropriate actions.

Recommendations:

We recommend that the Director, Minerals Management Service:

- 1. Evaluate acquiring system verification and auditing software.
- 2. Implement the system options to record activities in the SYSLOG during the system initialization process and develop and implement procedures to ensure that periodic reviews of the SYSLOG for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Program management.
- 3. Evaluate the available SMF record types and implement procedures to ensure that critical SMF logs are reviewed periodically and that Program management addresses the problems identified.

Minerals Management Service Response and Office of Inspector General Reply

In its response, the Service indicated agreement with Recommendations 2 and 3. However, the Service needs to provide additional information for Recommendations 2 and 3 and needs to reconsider its response to Recommendation 1, which is unresolved (see Appendix 3).

Recommendation 1. Nonconcurrence.

Service Response. The Service stated that the Program "routinely uses a number of system-assurance mechanisms such as control reports, system-assurance programs and user-reconciliation reports" but that it "remains alert to any technologic developments that would improve system integrity and operations." The Service further stated, "As these packages become available, they will be examined for applicability to the RMP [Royalty Management Program] computing environment."

Office of Inspector General Reply. The mechanisms cited by the Service provide information related mainly to application processing system assurance. Although the Service said that it will evaluate the use of software packages to assist in providing assurance over system integrity and operations, the Service should state concurrence or nonconcurrence with the recommendation to evaluate the acquisition of operating system-verification and auditing software that would identify mainframe operating system security exposures.

SERVICE CONTINUITY

M. Disaster Recovery Plans

Condition: Local area networks and personal computers used by the Program's divisions

that maintain proprietary and financial data were not included in the Program's

disaster recovery plans.

Criteria: Office of Management and Budget Circular A-130, Appendix III, states that

agencies should establish a contingency plan and periodically test the plan to ensure that operations will continue in the event that automated systems fail.

Cause: Program management did not ensure that all systems which maintain

proprietary and financial data were included in its disaster recovery plans.

Effect: If the disaster recovery plans are incomplete because all sensitive systems are

not included, personnel required to perform the disaster recovery procedures may not be able to recover critical systems in the event of a disaster or a system

failure.

Recommendation:

We recommend that the Director, Minerals Management Service, update the disaster recovery plans to include all mission-critical systems.

Minerals Management Service Response and Office of Inspector General Reply

Based on the Service's response, we request that the Service provide additional information for the recommendation (see Appendix 3).

Additional Comments on Finding

The Service stated, "We believe the disaster recovery plans we have in place for our mainframe and client servers provide coverage for virtually all of our mission-critical applications." In our opinion, this statement implies that disaster recovery plans are not required for other components of the Program's automated information system, such as local area networks and personal computers used by the Program's divisions. The local area networks and personal computers used by the Program's divisions were the components of the automated information system used to develop the Program's financial statements and

SERVICE CONTINUITY

to report financial information to the U.S. Treasury and the Office of Management and Budget. Further, these components also support the Program's mission to accurately and timely disburse rents, bonuses, and royalty revenues to the U.S. Treasury, the states, and the Indian tribes. Therefore, we believe that these components not only are "mission critical" to the Program but also are part of the Program's general support system. Office of Management and Budget Circular A-130, Appendix III, defines general support systems as "an interconnected set of information resources under the same direct management control which shares common functionality." Further, the Circular addresses the need for continuity of support for general support systems as well as major applications.



United States Department of the Interior

MINERALS MANAGEMENT SERVICE Washington, DC 20240

JAN 16 1998

Memorandum

To:

Assistant Inspector General for Audits

Through: Bob Armstrong

JAN 2 1 1998

From:

Cynthia Quarterman

Assistant Secretary for

Acting Director, Minerals Management Ser

Subject:

Office of Inspector General Draft Audit Report A-IN-MMS-001-97, "General

Controls Over the Automated Information System, Royalty Management

Program, Minerals Management Service"

Thank you for the opportunity to respond to this draft report on the general controls over our royalty automated information system. Of the 24 Recommendations, we agree with 11, partially agree with 2, and disagree with 11. We're sending you our general comments on the audit findings and specific ones on the recommendations. We've also included nine Enclosures to our response as additional background material for your review.

Please contact Bettine Montgomery at (202) 208-3976 if you have any further questions.

Attachments

MINERALS MANAGEMENT SERVICE RESPONSE TO DRAFT AUDIT REPORT "GENERAL CONTROLS OVER THE AUTOMATED INFORMATION SYSTEM, ROYALTY MANAGEMENT PROGRAM, MINERALS MANAGEMENT SERVICE"

Audit Agency: Office of Inspector General (OIG)

Audit Number: A-IN-MMS-001-97

We appreciate the opportunity to comment on this draft report. MMS shares OIG's concern for security and controls and concurs with some of the findings and recommendations presented in the report. In fact, the Royalty Management Program (RMP) is actively implementing solutions to rectify some of the weaknesses pointed out by the OIG and to enhance system security. We concur with OIG's use of OMB Circular A-130 as the principal criteria for evaluation; however, we cannot agree with OIG's implicit conclusion that RMP systems do not comply with the Circular. It is important to recognize these criteria are general, leaving considerable room for judgement and interpretation based on the individual facts and circumstances.

We indeed believe RMP systems are in substantial compliance with the spirit and intent of the OMB Circular and strenuously disagree with the overall conclusion of the report -- that general controls were inadequate. The OIG review identified some spot failures and procedural weaknesses, many of which we have agreed to change. However, in terms of materiality, the sum total of these weaknesses, in our opinion, is not significant enough to constitute an overall finding of inadequate. Furthermore, the report does not actually deal with the overall or general controls. To do so would require an evaluation of redundant and compensating controls. Yet, the OIG report stated "we did not evaluate the effectiveness of manual control procedures that may have operated as compensating controls for the automated information system general controls."

MMS would also point out that our recurring management control reviews have addressed such manual controls and generally found they were working effectively or prompted corrective actions to resolve minor control deficiencies. While these reports, as well as the supporting workpapers, were reviewed during this and prior OIG audits of our automated system, no adverse findings in this regard were reported. Moreover, past OIG audits performed under the Chief Financial Officers Act of 1990 have covered these controls, and each report concluded that our financial information was reliable.

We must dispute many of the OIG's facts, conclusions, and interpretations. System security is a complex network of redundant measures and policies which must strike an appropriate balance between risk and cost. Taken together, this network provides overall security for the key operating systems. No system is perfect, especially given the rapidly changing technological environment and the competing needs for funds. However, we believe OIG is holding RMP to

an unattainable standard in concluding general controls were "not adequate." MMS has established and continues to improve on a system of security controls that we believe should instead be viewed as a positive example, or even a model within the government.

Finally, the OIG report does not demonstrate a single negative impact of its findings. The OIG reported no incidents -- no loss or corruption of data and no theft or unauthorized access. We believe the absence of such incidents reflects favorably on our existing automated and manual compensating controls. Our primary comments on the facts and conclusions are shown below by topic. Additional comments on the facts and conclusions are included in our comments on the recommendations.

RISK ASSESSMENTS

MMS believes the risk assessment criteria were not appropriately applied. Circular A-130 states "The Appendix no longer requires the preparation of formal risk analyses" and that risk assessments "can be formal or informal, detailed or simplified, high or low level, quantitative (computationally based) or qualitative (based on descriptions or rankings), or a combination of these. No single method is best for all users and all environments." Given the breadth of judgement allowed on this matter, RMP's previous risk assessment documents and processes were clearly in accordance with the guidelines. We must also disagree with OIG's findings that MMS did not properly assess the risks regarding year 2000 program conversion, "unsupported" system security software, and "geopolitical" and "external directives" risks.

In 1996, RMP management anticipated the potential risks associated with the Year 2000 conversion and tasked its operations and maintenance contractor to conduct a detailed analysis of major systems and develop a plan for modifying and testing the programs. The resultant \$1.6 million project was begun by the contractor in March 1997 and is on track for completion in 1998. (Enclosures 1, 2, 3 and 4). In May 1997, RMP management also initiated a parallel internal project to assess non-mainframe, stand-alone systems. Given the fact that OMB Circular A-130 does not even require formal risk analyses; it would seem that such an explicit recognition of this risk and timely action toward its elimination is as an accomplishment rather than a failure.

We also believe the OIG misunderstood the circumstances involving the "Resource Access Control Facility" (RACF) mainframe security software. The system-security software was never "unsupported" in the sense implied by OIG; this was a contractual matter that would have required a paid service call rather than a supported call if a problem arose. Because RMP was planning to upgrade to a different operating system, we chose not to incur the expense of a software upgrade at that time. RMP was never at any risk regarding this software.

We also take issue with OIG's opinion regarding our assessment of "geopolitical" and "external directives" risks. In our view, OIG's opinion that RMP was at risk of employee sabotage because of low morale associated with potential program abolishment or downsizing is overstated. Since the program's inception in 1982, RMP employees have become accustomed to such proposals. While they may indeed weaken morale, we have learned external threats are more likely to rally our employees than to foster mischief. While we consider the employee morale issue to be important matter, RMP correctly assessed this risk as "low."

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

RMP disagrees with OIG's statement that "Program management did not have procedures to ensure that client/server application software changes were authorized, approved, and tested before being moved into production." Such procedures have been in place since 1995 and are published in an on-line help text format (Enclosure 5). The Client/Server Guidelines clearly define the steps/processes for testing to be included in the Implementation Plan (part of the Visualization Step) and the Unit, System, and User Testing required as part of the Operational Prototype (Development Step). These Guidelines include a separate Procedural Overview of Testing including an example test plan. While testing processes for client-server applications are different from those for mainframe systems because of the emphasis on interactive prototyping and Graphical User Interface design, they are no less adequate.

DEFAULT SETTINGS

The OIG found one instance where a default ID provided with off-the-shelf software was not removed as required. However, it is factually incorrect to say that use of this default ID allows access to all mainframe computer resources. The security architecture prevented any unauthorized or inappropriate user from using this ID because users must first be able to access the system through a valid RACF logon password and have a user ID defined to the data dictionary. At no time were RMP resources at risk

SECURITY SOFTWARE

The OIG seems to have misunderstood the reasons for and the effects of RMP's decision not to upgrade RACF, the commercial mainframe security software. As noted above, RMP initially delayed the upgrade because it was considering a processor replacement that would require an entire new suite of mainframe software products. Upgrading RACF at that time would have been an inherently risky and potentially expensive decision. Moreover, the current version of RACF had been very stable. The only risk of running "unsupported" software is contractual; that is, in the unlikely event of a RACF failure, IBM would have to be called in for service on demand rather than as a fully supported maintenance call.

DISASTER RECOVERY PLANS

The OIG seems to have generalized two distinct concepts and used them interchangeably. Sensitive or proprietary information is not synonymous with mission critical-systems and information. Although most MMS mission-critical information is sensitive, the reverse is not the case. Most sensitive data is not mission critical.

The central repository for mission-critical information resides on the mainframe computer. This is where MMS's key systems reside--the heart of the MMS' operations--requiring a comprehensive disaster recovery plan. Users know they can always go to this central repository for the official and current data. This database is updated continuously, centrally managed, and routinely backed up. Because most of this data is also business-sensitive, security controls are also in place to prevent unauthorized disclosure.

In addition, large amounts of redundant data reside in paper and electronic format in and on desks, file cabinets, and personal computers. This includes sensitive and financial data. However, because most of this data is redundant, it is not "mission critical." Therefore, while it is important to prevent unauthorized disclosure of this information, disaster recovery plans are, in most cases, not cost effective, feasible, or necessary.

Therefore, OIG's conclusion that disaster recovery plans are needed for all local area networks and personal computers that contain proprietary and financial data is erroneous. We believe the disaster recovery plans we have in place for our mainframe and client servers provide coverage for virtually all of our mission-critical applications. We are currently reviewing "stand alone" PC systems to determine if any are truly mission critical. If so, they will need to be brought onto the network and managed accordingly.

COMMENTS ON RECOMMENDATIONS

A1. Ensure that risk assessments are conducted in accordance with guidelines, which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the assessments should address significant risks affecting systems, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of the residual risk.

DISAGREE - While MMS plans to enhance and better document our risk assessment process due to the rapidly changing computing and communication environment, we believe our previous assessments were in accordance with guidelines.

A2. Formally assign and communicate responsibility to local area network administrators to participate in risk assessments and ensure compliance with the Program's security policy.

DISAGREE - RMP policies define the LAN administrators' role in contingency planning and security. (Enclosure 6).

A3. Determine the risks associated with local area network applications and personal computer databases that contain proprietary and financial data and, based on the results of the risk assessments, establish appropriate security policies and procedures.

AGREE - RMP will conduct a risk analysis on user written applications as well as data residing on networks and personal computers to determine appropriate security and disaster recovery procedures. An inventory of these applications and the business functions they support is already being performed as part of RMP's Year 2000 project.

B1. Evaluate Systems Management Division and contractor ADP positions to determine position sensitivity in relation to risk and ADP factors. Also, assurance should be provided that automated information system work is technically reviewed by persons whose position sensitivity level is greater than the position sensitivity levels of the employees who are performing the work.

PARTIALLY AGREE - We plan to reevaluate the position sensitivity level for the senior personnel in charge of the contractor activity to determine if those position should be classified at a higher level. In accordance with Departmental criteria, most ADP staff are designated noncritical sensitive. We doubt it was the OIG's intention to imply that *all* work must be reviewed by persons at a higher sensitivity level; however, this would be impossible in a multiple level organization because there are only two sensitivity levels from which to choose, i.e., "noncritical-sensitive" and "critical-sensitive."

B2. Establish controls to ensure that the contractor is fulfilling its contractual obligation of submitting requests for background checks within the specified time frame and that contractor employees who are in probationary status and awaiting security clearances are not performing critical ADP work.

PARTIALLY AGREE - We agree controls are needed to assure the contractor timely submits requests for background checks. The contractor has been directed and has begun to track and is accountable for the status of its submission of these requests. We also agree that employees awaiting clearances should be in probationary status; however, it would be unacceptably costly to prohibit employees from performing critical ADP work. Except for positions which require access to information dealing with national security, all Federal employees are hired and perform

the full scope of their jobs while the appropriate investigation is conducted and a suitability determination is made. We believe a similar criterion is appropriate for our contractors. Most all software development and system operation work could be considered critical. As a practical matter, we could not delay replacing contractor employees in such work pending the completion of background checks. However, we are exploring alternatives with the contractor such as having them perform a preliminary "criminal and credit check" which is quick and inexpensive.

B3. Establish controls to ensure that personnel or security files accurately reflect that background checks and periodic follow-up background checks are performed as required.

DISAGREE - Controls are already in place to ensure that personnel or security files accurately reflect background checks. MMS's Office of Administration and Budget maintains documentation and a tracking system on all MMS employee and contractor security clearances and background checks. We also disagree with the OIG's statement that followup background checks are required. MMS is in compliance with Departmental guidance (Enclosure 7) that followup checks are authorized *only* for national security positions and not for public trust positions.

C1. Establish controls to enforce Program policy that requires employees to sign security awareness statements before their access to system resources is approved by the Installation Automated Information System Security Officer.

AGREE - While our own test sample has confirmed that our users have appropriate access to RMP systems, we concur that our filing system for access approvals needed improvement. All statements are now consistently filed and reconciled by the ADP security officer.

D1. Ensure that individual computer resources are classified based on the level of sensitivity associated with each resource.

DISAGREE - We believe our current classifications are appropriate. Most RMP data is sensitive or "proprietary" and must be protected from unauthorized disclosure. Our mainframe systems receive heightened security because they are more mission critical, not because they are more sensitive. As explained in previous segments, these systems must be protected more strenuously to ensure the integrity of the official records.

A more moderate level of protection is necessary for proprietary information than for mission critical information. The umbrella protection mechanism for all types of proprietary information is physical controls coupled with employee training. RMP works in a secure environment and trains employees to protect all forms of proprietary information such as paper copies, information on their PC's, and floppy disks, in addition to information which resides on networks and

servers. While it would be possible to install network security measures equivalent to the mainframe measures, we believe the significant additional cost would not be justified. We believe the protection level over all proprietary information is appropriate.

The OIG is technically correct in its statement that MMS had not officially designated any of its systems as "major". However, RMP has <u>treated</u> its mission-critical mainframe applications as major (as allowed by OMB Circular A-130) by providing extra security controls and disaster recovery capabilities. Based on our interpretation of A-130, the fact that these systems were not officially designated as major systems in our annual security plan is incidental and not substantive.

D2. Evaluate controls over resources to ensure that the access controls have been implemented commensurate with the level of risk and sensitivity associated with each resource.

DISAGREE - We believe our existing access controls over resources already meet the intent of this recommendation. All MMS employees are granted access to view royalty, production, and reference data. Since most of this data is proprietary, employees are trained in its proper use and must sign statements acknowledging their responsibility to protect it. State and Tribal employees have access to such data within their jurisdictions only. The ability to add or change data is limited to those employees who require that access to perform their jobs.

E1. Implement controls to enforce Program policy that default user ID's and passwords are to be removed from the automated information system when commercial off-the-shelf software is implemented.

AGREE - The contractor has implemented a verification procedure to ensure this situation does not recur.

F1. Evaluate the current Program policy which only recommends that passwords contain a mix of letters and numbers for all automated information system components. Implement, if the Program determines that a mix of letters and numbers should be required, the security software option within RACF that would enforce this requirement. If the Program determines that a mix of letters and numbers is not required, the risk should be addressed in the risk assessment.

AGREE - RMP will assess this issue and document the decision.

F2. Develop and implement centralized security administration for the local area networks used by the Program's divisions that contain proprietary and financial data.

AGREE - We are in process of implementing centralized security administration for efficiency purposes. However, we cannot support OIG's basis for this recommendation, i.e., that "... no Program procedures were in place to ensure that controls were adequate to safeguard these local area networks and personal computers" as evidenced by two allegedly inappropriate software settings. As discussed below, we disagree the settings are inappropriate. RMP has had security and recovery procedures in place for its LAN's since 1993, and the fileservers are secure.

F3. Change the "SET UNENCRYPTED PASSWORD" to "OFF" and include the "SECURE CONSOLE" command in the AUTOEXEC.NCF file on all file servers to prevent users from gaining unauthorized access to sensitive files.

DISAGREE - RMP was aware of the software settings issues suggested by the OIG and had consciously decided to leave the settings as they are. In both cases, the judgements were based on operational issues, taking risk into consideration. The limited security exposure was mitigated by the physical controls. The servers in question are in a locked LAN room within a controlled access building. Both of these decisions fall under the security judgement mandated by the A-130 and the National Institute of Standards and Technology (NIST) handbook which states that "The costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits". It was RMP's judgement that the real costs of setting these parameters in the way suggested by OIG clearly exceeded their limited security benefits.

G1. Implement controls to ensure that access managers approve all access to their applications in accordance with Program policy.

DISAGREE - We believe effective controls have been in place to assure that application managers approve all access to their applications (see Enclosure 7). We acknowledge that our filing system for such approvals needed improvement and are in the process of resolving this problem.

G2. Document procedures which require that users' access levels be reviewed periodically or that employees be re-certified to ensure that the levels of access granted are appropriate for the duties assigned to the users.

AGREE - We concur with the need to document these procedures. However, we disagree with the OIG's implication (in its statement of effect) of any significant risk of security breaches. Access to mission-critical systems has been carefully managed and controlled through documented security procedures and controls, including mainframe access matrices and annual reviews by the Security Manager. Our own tests confirmed that no unauthorized access exists or has existed.

H1. Evaluate the need to deviate from the Departmental standard for the number of unsuccessful log-in attempts. If the Program determines that this number should remain at five, Program management should request, from the Department, a waiver from the standard of three attempts.

AGREE - A DOI waiver for RMP to extend the password attempts from three to five for the RMP was granted on November 14, 1997. (Enclosure 9)

I1. Document procedures for authorizing, approving, and testing client/server application software before the software is moved into production.

DISAGREE - These documented procedures are already in place. (Enclosure 5)

J1. Implement controls to ensure that application programmers do not have access to the production client/server application data or the capability to update/change these data.

DISAGREE - While application programmers do not routinely require update access to any RMP production data, there are instances when temporary access is needed by specific programmers under controlled circumstances. To mitigate any future risks associated with this access, procedures have been reinforced which detail actions to be taken when requesting temporary access to mainframe and client/server production data. We also refute OIG's statement that application programmers serve as "backup" to end-users. This does not occur.

J2. Improve detection controls by ensuring that management or the Installation Security Officer reviews server security logs periodically.

AGREE - The contractor is being directed to address the review of server security logs within their overall internal control procedures. (We do not believe MMS management or the Installation Security Officer should carry out this procedure.)

K1. Ensure that the upgraded version of RACF is implemented immediately if the Program is granted waiver from consolidating its mainframe operations with another mainframe operation.

DISAGREE - As discussed under Risk Assessments (Page 2), we believe OIG misunderstood the effects of delaying this software upgrade. Although this is a moot point now that MMS has replaced its processor, the decision not to upgrade the RACF software was well founded.

L1. Evaluate acquiring system-verification and auditing software.

DISAGREE - RMP routinely uses a number of system-assurance mechanisms such as control reports, system-assurance programs and user-reconciliation reports. Nonetheless, RMP remains

alert to any technologic developments that would improve system integrity and operations. As these packages become available, they will be examined for applicability to the RMP computing environment.

L2. Implement the system options to record activities in the SYSLOG during the system initialization process and develop and implement procedures to ensure that periodic reviews of the SYSLOG for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Program management.

AGREE - System initialization activities as well as operator commands are already recorded in the SYSLOG. Because we are uncertain of the payoff and cost effectiveness of the periodic reviews, we will conduct a pilot test. The SYSLOG will be reviewed following system initialization for inappropriate and unauthorized activities that may have occurred during the test. Based on the results, we will assess the feasibility of fully implementing this routine.

L3. Evaluate the available System Management Facility (SMF) record types and implement procedures to ensure that critical SMF logs are reviewed periodically and that Program management addresses the problems identified.

AGREE - We have evaluated record types and concluded that certain log record types may be worthwhile for periodic review. We will pilot test a monthly review of these record types. Depending on the volume of records and the payoff, RMP will continue, expand, or reconsider this detection method. Program management will be notified when problems are identified.

M1. Update the disaster recovery plans to include all mission-critical systems.

AGREE - We plan to update the disaster recovery plans to include all mission-critical systems. However, we do not agree with the OIG's presumption that all systems containing proprietary or financial data are "mission critical." Many PC-based systems contain *copies* of such data for analysis, but these systems are not considered mission critical. MMS' ongoing Year 2000 project is identifying and classifying any stand-alone systems that managers judge to be "mission critical." If so, these systems will be reclassified as such and will be required to reside on LAN's or servers that can be centrally backed up for recovery purposes.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.1	Unresolved.	Reconsider the recommendation to clarify that the enhanced risk assessment process will include the identification of significant risks affecting systems, will appropriately identify controls implemented to mitigate those risks, and will formalize the acceptance of residual risk. Also, an action plan that includes target dates and titles of officials responsible for implementation should be provided.
A.2	Unresolved.	Reconsider the response to ensure that local area network administrators participate in the risk assessment process, and provide an action plan that includes target dates and titles of officials responsible for implementation.
A.3, F.1, F.2, L.2, L.3, and M.1	Management concurs; additional information needed.	Provide an action plan that includes titles of officials responsible for implementation.
B.1, B.2, E.1, and J.2	Management concurs; additional information needed.	Provide an action plan that includes target dates and titles of officials responsible for implementation.

Finding/Recommendation Reference	Status	Action Required
B.3, D.1, D.2, and L.1	Unresolved.	Reconsider the recommendations, and provide action plans that include target dates and titles of officials responsible for implementation.
C.1	Unresolved.	Provide information relating to how the reconciliation of the statements was performed and the dates the actions were completed.
G.1	Unresolved.	Reconsider the recommendation, and provide information regarding controls which ensure that all access managers approve all access to their applications. Also, an action plan that includes target dates and titles of officials responsible for implementation should be provided.
G.2	Unresolved.	Reconsider the recommendation, and provide information regarding documentation of procedures requiring users' access level reviews or recertification of users' access be performed periodically. Also, an action plan that includes target dates and titles of officials responsible for implementation should be provided.
H.1	Implemented.	No further action is required.

Finding/Recommendation Reference	Status	Action Required
I.1	Unresolved.	Respond to the revised recommendation, and provide an action plan that includes target dates and titles of officials responsible for implementation.
J.1	Unresolved.	Reconsider the recommendation, and provide the procedures that mitigate risks when application programmers are allowed update access to production data.
K.1	Unresolved.	Reconsider the recommendation, and provide information on whether the upgraded version of the security software has been implemented on the new processor.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

Within the Continental United States

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240 Our 24-hour Telephone HOTLINE 1-800-424-5081 or (202) 208-5300

TDD for hearing impaired (202) 208-2420 or 1-800-354-0996

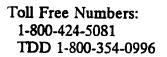
Outside the Continental United States

Caribbean Region

U.S. Department of the Interior Office of Inspector General Eastern Division - Investigations 1550 Wilson Boulevard Suite 410 Arlington, Virginia 22209 (703) 235-9221

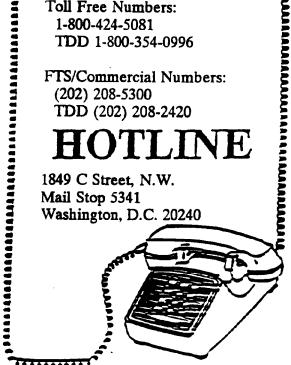
North Pacific Region

U.S. Department of the Interior Office of Inspector General North Pacific Region 238 Archbishop F.C. Flores Street Suite 807, PDN Building Agana, Guam 96910 (700) 550-7428 or COMM 9-011-671-472-7279



FTS/Commercial Numbers: (202) 208-5300 TDD (202) 208-2420

1849 C Street, N.W. Mail Stop 5341 Washington, D.C. 20240





U.S. Department of the Interior Office of Inspector General

AUDIT REPORT

GENERAL AND APPLICATION CONTROLS
OVER THE TECHNICAL INFORMATION
MANAGEMENT SYSTEM,
OFFSHORE MINERALS MANAGEMENT,
MINERALS MANAGEMENT SERVICE

REPORT NO. 00-I-647 AUGUST 2000

EXECUTIVE SUMMARY

General and Application Controls Over the Technical Information Management System, Offshore Minerals Management, Minerals Management Service Report No. 00-I-647 August 2000

BACKGROUND

The Minerals Management Service (MMS) manages the Nation's natural gas, oil, and other mineral resources on the Outer Continental Shelf and collects, accounts for, and disburses revenues from offshore and onshore mineral leases on Federal and Indian lands. MMS's Offshore Minerals Management (OMM) program manages the Outer Continental Shelf mineral leases. These leases result in more than \$4 billion of royalties being collected annually. Also, OMM provides oversight to ensure safe and environmentally sound exploration and production of the Nation's mineral resources on the Outer Continental Shelf. To accomplish its mission and to automate business and regulatory functions, OMM designed, developed, and implemented the Technical Information Management System (TIMS), an MMS mission-critical system and a comprehensive corporate database.

OBJECTIVE

The objective of the audit was to determine whether OMM had effective general and application controls over TIMS and whether TIMS was operated in compliance with applicable Federal laws and regulations. In addition, we performed this audit to support the Office of Inspector General's examination of the financial statements of MMS by evaluating the reliability of the controls over computer-generated data that support the Royalty Management Program's portion of the financial statements.

RESULTS IN BRIEF

Overall, we concluded that OMM had established adequate general and application controls over TIMS. However, improvements are needed in four areas in OMM's general and application controls over TIMS. These areas are the security program, the continuity of operations plan to protect data in the event of a disaster or a system failure, controls over access to TIMS data, and software development and change management. Federal laws and regulations and Department of the Interior and MMS policies and procedures require that general and application controls be established and implemented to protect information in computer systems. Weaknesses existed in the controls over TIMS because OMM management had not developed an adequate security program and had not ensured that policies and procedures were followed. The lack of adequate controls increased the risk

that TIMS data could be accessed and modified or disclosed by unauthorized users, that TIMS software and data could be stolen or destroyed, that TIMS functions and processes could not be recovered in the event of a disaster or a system failure, and that TIMS could not perform as intended.

RECOMMENDATIONS

We made 15 recommendations related to MMS's controls over TIMS. These recommendations related to improving (1) OMM's security program over TIMS, (2) TIMS' continuity of operations plan, (3) access controls to TIMS and its databases, and (4) the policies and procedures for making changes to TIMS software and for testing the changes.

AUDITEE COMMENTS AND OIG EVALUATION

MMS concurred with the report's 15 recommendations. Based on the response, we considered eight recommendations resolved and implemented and seven recommendations resolved but not implemented.



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

AUG 3 / 2000

AUDIT REPORT

Memorandum

To:

Director, Minerals Management Service

From:

Roger La Rouche

Acting Assistant Inspector General for Audits

Subject: Audit Report on General and Application Controls Over the Technical

Information Management System, Offshore Minerals Management, Minerals

Management Service (No. 00-I-647)

INTRODUCTION

This report presents the results of our review of general and application controls over the Minerals Management Service's (MMS) Technical Information Management System (TIMS). The objective of the audit was to determine whether MMS had effective controls over TIMS and whether TIMS was operated in compliance with applicable Federal laws and regulations. In addition, we performed this audit to support the Office of Inspector General's examination of the financial statements of MMS by evaluating the reliability of the controls over computer-generated data that support the Royalty Management Program's portion of the financial statements.

BACKGROUND

MMS manages the Nation's natural gas, oil, and other mineral resources on the Outer Continental Shelf and collects, accounts for, and disburses revenues from offshore and onshore mineral leases on Federal and Indian lands. In 1998, MMS collected \$5.6 billion from Federal and Indian mineral leasees, of which \$4.3 billion was from Outer Continental Shelf mineral leasees. MMS has two specialized operating programs, the Offshore Minerals Management (OMM) program and the Royalty Management Program. OMM manages the Outer Continental Shelf mineral leases and provides oversight to ensure the safe and environmentally sound exploration and production of the Nation's mineral resources on the Outer Continental Shelf. OMM has its headquarters in Washington, D.C., with offices in Herndon, Virginia, and has regional offices in New Orleans, Louisiana; Anchorage, Alaska; and Camarillo, California. Also, the headquarters OMM Leasing Division has its Mapping and Boundary Branch, located in Denver, Colorado. The Royalty Management Program manages the accounting for and the collection and disbursement of royalty, rent, and bonus revenues generated from Federal and Indian mineral leases.

To accomplish its mission, OMM designed, developed, and implemented TIMS, an MMS mission-critical system and a comprehensive corporate database that replaced and upgraded all Federal information processing resources which supported the OMM program. TIMS was developed to modernize and replace several critical offshore systems, including the Outer Continental Shelf Information System, the Offshore Inspection System, the Automated Cartographic System, and the Geological and Geophysical Database. TIMS information is used, in part, to update the Royalty Management Program system with oil and gas well production data from offshore leases to assist in verifying the accuracy of royalties collected from the Outer Continental Shelf.

TIMS is a computerized information system that automates all business and regulatory functions of OMM. TIMS is a three-tier¹ client/server platform with application servers located at all the OMM regional offices (three) and district offices (six) and database servers located at the regional offices. The Chief of the OMM Information Technology Division is the owner of TIMS. The Division is responsible for developing and maintaining TIMS's database structures, and regional and district offices are responsible for the data in the databases. TIMS employs the Oracle relational database management system and tools to manage data and support OMM business functions. In addition, TIMS includes commercial off-the-shelf software for OMM geologic interpretative tools and mapping functions. TIMS is constructed of 41 business components² (the components are listed in Appendix 2), which include more than 800 modules. To operate, TIMS uses approximately 55 different types of hardware items, such as personal computers and network equipment, and 68 software items, such as Windows NT and UNIX operating systems, ArcView, Geoquest, and Microsoft Office.

SCOPE OF AUDIT

We reviewed OMM general and application controls over TIMS. Specifically, we reviewed the following general controls: (1) software development and change management, (2) risk assessment, (3) security plans, (4) service continuity, (5) system software, and (6) access controls. For application controls, we reviewed input, processing, authorization, and output.

¹A three-tier client/server environment is defined as one in which "the user interface is stored in the client, the bulk of the business application logic is stored in one or more servers, and the data are stored in a database server." (The Computer Language Company, Inc., Computer Desktop Encyclopedia, 1981-1999)

²TIMS is divided into major groupings or components that correspond to the different activities overseen by OMM.

To accomplish our objective, we interviewed OMM and contractor personnel, reviewed application and systems documentation, observed and became familiar with system operations and data structures, analyzed access and security controls, and evaluated service continuity procedures and testing. The audit was conducted at the Information Technology Division Office of OMM and the OMM Gulf of Mexico Regional Office in New Orleans and Division headquarters and the Information Management Division in Herndon. Although TIMS is installed at all of the regional offices, our review was limited to the Gulf of Mexico Regional Office because this regional office processes almost 90 percent of the data related to oil and gas production and Outer Continental Shelf royalties.

Our audit was made in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we employed statistical test samples to determine the adequacy of TIMS access controls and software development and change management procedures. Specifically, we randomly selected 77 TIMS users from a list of 849 users who had access to TIMS. Also, we randomly selected 132 change requests from a list of 1,157 change requests for the period of October 1998 through June 1999.

During our audit, the Department of the Interior's Office of Information Resources Management contracted to acquire professional services to support the Department with testing, analysis, and vulnerability assessment of Departmentwide information technology architecture. Specifically, the contractor was tasked with performing a comprehensive vulnerability analysis (using Internet Security Systems scanning software) of Departmental internet protocol address assignments, which included OMM internet protocol addresses. As a result, we did not review the results of the analysis of OMM networks.

PRIOR AUDIT COVERAGE

During the past 5 years, neither the General Accounting Office nor the Office of Inspector General has issued any reports related to OMM's general and application controls over TIMS.

RESULTS OF AUDIT

We concluded that overall, MMS's OMM had established adequate general and application controls over TIMS. However, we believe that the general controls of OMM need improvements in four areas: security program; continuity of operations in the event of a disaster or a system failure; controls over access to TIMS; and software development and change management. Office of Management and Budget Circular A-130, "Management of Federal Information Resources," and National Institute of Standards and Technology publications and guidelines require agencies to establish and implement computer security

and management and internal controls to improve the protection of sensitive³ information in the computer systems of executive branch agencies. Additionally, the Congress enacted laws, such as the Privacy Act of 1974 (5 U.S.C. § 552a) and the Computer Security Act of 1987 (40 U.S.C. § 759), to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls over sensitive information is adequate. Further, the Department of the Interior and MMS have issued policies and procedures to implement general and application controls to protect sensitive data in automated information systems. Weaknesses existed in the general controls over TIMS because OMM management had not developed an adequate security program and had not ensured that policies and procedures were followed. The lack of adequate controls may increase the risk of (1) unauthorized access and modifications to and disclosure of sensitive TIMS data, (2) theft or destruction of OMM software and sensitive information, (3) loss of TIMS systems and functions in the event of a disaster or a system failure, and (4) TIMS not performing as intended.

In the four areas that needed improvements in the controls, we identified 8 weaknesses and made 15 recommendations for improving the controls over TIMS. The weaknesses are summarized in the paragraphs that follow, and details of the weaknesses and our respective recommendations to correct these weaknesses are in Appendix 1.

Security Program

OMM management did not have a security plan for TIMS and did not ensure that computer security awareness training was provided. As a result, there was an increased risk that sensitive data could be impaired or compromised and that data could be inadvertently disclosed or destroyed or erroneously modified. We made three recommendations to correct these weaknesses.

Service Continuity

OMM's contingency planning, backup, and disaster recovery procedures did not provide reasonable assurance that the TIMS processing environment could be recovered in the event of a disaster or a system failure. Specifically, the Continuity of Operations Plan had not been tested, critical personnel had not been trained to effectively implement the Plan, a copy of the Plan was not kept at the off-site storage facility, and TIMS data and applications were not routinely transferred to the off-site storage facility. As a result, there was an increased risk that the mission-critical TIMS could not be recovered in the event of a disaster or a system failure. We made five recommendations to address these weaknesses.

³"Sensitive data" is defined in 40 U.S.C. § 759 as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act)."

Access Controls

OMM management did not limit the numbers of log-in attempts allowed for access to TIMS, did not control password settings, did not remove in a timely manner access for employees who terminated their employment, and did not control access to TIMS databases. As a result, there was an increased risk that sensitive data maintained on TIMS were vulnerable to unauthorized access, manipulation, and disclosure. We made four recommendations to address these weaknesses.

Software Development and Change Management

OMM management did not implement controls to ensure that TIMS application software changes were authorized, approved, and tested before being moved into production. As a result, there was an increased risk that TIMS applications may not perform as intended. We made three recommendations to address these weaknesses.

MMS Response and Office of Inspector General Reply

In the July 19, 2000 response (Appendix 3) to the draft report from the Director of MMS, MMS concurred with all of the 15 recommendations. Based on the response, we consider Recommendations C.1, C.3, C.4, D.1, D.2, E.1, F.1, and G.1 resolved and implemented and Recommendations A.1, B.1, B.2, C.2, C.5, G.2, and H.1 resolved but not implemented. Accordingly, the unimplemented recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

Although MMS concurred with Recommendation H.1, it disagreed with the "analysis that MMS stated that although the TIMS drew the auditors to the recommendation." Maintenance Methodology required test plans, the test plans were not required for "routine and/or minor changes," such as reports, system administration functions, database triggers, software packages, and menu changes. We believe that testing is a critical component of software maintenance because testing ensures that applications meet user and management needs, produce reliable data, and operate in accordance with laws, regulations, and management policies and procedures. Test plans should define the expected output and include tests for valid, invalid, expected, and unexpected results. The TIMS Maintenance Methodology does not allow for exceptions from change management procedures such as testing for system administration, database triggers, software packages, and menu changes. Further, the TIMS Maintenance Methodology does not allow for exceptions to exclude the quality assurance group and user group from testing changes prior to the changes being moved into production. The Methodology states that "every TIMS work product must pass quality assurance tests before made available for testing by the Customer User Acceptance Team."

Since the report's recommendations are considered resolved, no further response to the Office of Inspector General is required (see Appendix 4).

Section 5(a) of the Inspector General Act (5 U.S.C. app. 3), requires the Office of Inspector General to list this report in its semiannual report to the Congress. In addition, the Office of Inspector General provides audit reports to the Congress.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

SECURITY PROGRAM

A. Computer Security Plan

Condition:

Offshore Minerals Management (OMM) had not developed a security plan for the Technical Information Management System (TIMS), which has been identified by the Minerals Management Service (MMS) as a sensitive and mission-critical system.

Criteria:

Security plans are required by 40 U.S.C. § 759 and Appendix III, "Security of Federal Automated Information Resources," of Office of Management and Budget Circular A-130, "Management of Federal Information Resources," to be developed for all sensitive computer systems. A computer security plan is designed to assist agencies in addressing the protection of general support systems and major applications that contain sensitive information to help ensure the system's integrity, availability, and confidentiality. In addition, National Institute of Standards and Technology's (NIST) Special Publication 800-18. "Guide for Developing Security Plans for Information Technology Systems," provides guidance on developing, implementing, and monitoring security plans for automated information systems. Also, Appendix III of Circular A-130 requires that a summary of the security plan be incorporated into the agency's Strategic Information Resources Management Plan. Additionally, Appendix III of Circular A-130 states that the lack of a security plan for a major application should be considered a deficiency pursuant to Office of Management Budget Circular A-123, "Management Accountability and Control," and the Federal Managers' Financial Integrity Act (31 U.S.C. § 1105, 1113, and 3512).

Cause:

OMM information technology officials did not ensure that a computer security plan for TIMS was prepared in accordance with 40 U.S.C. § 759, Office of Management and Budget requirements, and NIST guidelines. According to OMM officials, a draft TIMS Y2K (Year 2000) contingency plan was prepared that addressed degradation or failure of activities and remedies should any event threaten or disable the system. However, this plan did not meet the requirements for a security plan because it did not include the rules of the system, such as rules of behavior concerning use of, security in, and acceptable level of risk for the system; training of all individuals on their security responsibilities; personnel controls; incident response

SECURITY PROGRAM

capability; continuity of support; technical security; and identification of connections to other systems.

Effect:

Without this plan, OMM did not have adequate assurance that data in its TIMS were adequately protected.

Recommendation

We recommend that the Director of MMS ensure that a computer security plan for TIMS is developed, implemented, and monitored in accordance with the United States Code, Office of Management and Budget Circular A-130, and NIST guidelines.

SECURITY PROGRAM

B. Computer Security Training

Condition:

Mandatory computer security awareness training had not been provided to OMM employees and contractor personnel. Specifically, at least 220 Gulf of Mexico Regional Office and district personnel and Information Technology Division personnel had not received annual computer security awareness training since 1992.

Criteria:

Mandatory periodic training in computer security awareness and accepted computer security practices is required by 40 U.S.C. § 759 for employees who are involved in managing, using, or operating each Federal computer system within or under the supervision of that agency. In addition, the Department of the Interior's "Automated Information Systems Security Handbook" requires that computer security training be provided on an ongoing basis and that refresher training be provided at least annually.

Cause:

OMM information technology officials had not established policies and procedures to ensure that annual computer security awareness training was completed in accordance with applicable computer security guidelines.

Effect:

Without annual training in computer security awareness and accepted computer security practices of employees who are involved in managing, using, or operating sensitive OMM computer systems, including TIMS, there is an increased risk of unauthorized disclosure of sensitive and propriety data.

Recommendations

We recommend that the Director of MMS:

- 1. Implement policies and procedures to ensure that OMM employees and contractor personnel who are involved with sensitive component systems receive annual computer security awareness training.
 - 2. Ensure that training is documented in the employee human resource files.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

C. Service Continuity

Condition:

OMM did not have an effective means of recovering or continuing critical TIMS functions and operations in the event of a system failure or a disaster. Specifically, we found that:

- The Gulf of Mexico Region's April 1996 Continuity of Operations Plan had not been tested to ensure that the planned procedures for recovering TIMS and other business functions were feasible.
- Although Gulf of Mexico regional management had developed a draft plan, dated September 1999, neither the draft plan nor the April 1996 plan included recovering critical TIMS development and maintenance functions of OMM's Information Technology Division.
- Regional personnel responsible for continuing critical functions in the event of a disaster or an emergency were not trained in their roles and responsibilities described in the Continuity of Operations Plan.
- A copy of the Plan was not available at the designated off-site storage facility.
- Neither regional nor Information Technology Division personnel ensured that backup tapes of critical TIMS data and applications were routinely transferred to the off-site storage facility.

Criteria:

Appendix III of Circular A-130 requires agencies to establish controls to safeguard all information processed, transmitted, or stored in Federal automated information systems. Further, the Circular requires agencies to establish a contingency plan and periodically test the plan for the capability to perform the agency function supported by the application in the event of failure of its automated support. In addition, NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," recognizes that the success of recovering all information systems operations and data is largely dependent upon the adequacy of contingency planning, including backup and recovery procedures and testing of the plans; requires that personnel be trained in their contingency-related duties; and requires that contingency plans be stored in a safe place. The Department of the Interior's "Automated Information Systems Security Handbook" and the MMS Manual mandate routine cyclical off-site storage for all automated information

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

systems data and applications providing critical support to the organization's mission.

Cause:

OMM information technology officials did not ensure that adequate service continuity controls were in place for critical TIMS functions and operations to continue without undue interruption if unexpected events occurred, such as a system failure. In addition, OMM management did not ensure that critical and sensitive TIMS application components and data were protected by being stored off-site on a routine cyclical basis.

Effect:

In the event of a disaster or a system failure, OMM was at risk of not being sufficiently prepared to recover critical TIMS functions and continue critical operations.

Recommendations

We recommend that the Director of MMS:

- 1. Develop a Continuity of Operations Plan for the Offshore Minerals Management Information Technology Division, which includes procedures for recovery of the Division's critical TIMS functions.
- 2. Periodically test the Continuity of Operations Plan and update the Plan based on the test results.
- 3. Ensure that copies of the Continuity of Operations Plan are maintained at the off-site facility.
- 4. Ensure that backup copies of TIMS applications, components, and data are stored at the off-site storage facility on a routine cyclical basis.
- 5. Provide training to OMM personnel who are responsible for the recovery of critical TIMS business functions and operations about their roles and responsibilities related to the Continuity of Operations Plan.

SYSTEM ACCESS CONTROLS

D. User Access

Condition:

OMM did not adequately control access to TIMS databases. Specifically, employees who were no longer employed by MMS still had access to TIMS. For example, we found that 28 percent of employees who had terminated their employment still had access to the TIMS Gulf of Mexico regional production database; 6 percent of departed employees, including the prior Database Administrator, had access to the TIMS development database; and 13 percent of departed employees had access to the TIMS Customer User Acceptance Team, the testing database. In addition, 798 users had access to the Customer User Acceptance Team's database when there were only 79 team members who were authorized to access the database.

Criteria:

NIST's Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," states:

It is necessary to periodically review user account management on a system. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, [and] whether management authorizations are up-to-date.

Cause:

OMM Gulf of Mexico regional and Information Technology Division officials did not ensure that controls were in place to delete employee access to TIMS when employees departed the organization.

Effect:

As a result, the risk was significantly increased that unauthorized users could gain access to sensitive and mission-critical TIMS data and applications.

Recommendations

We recommend that the Director of MMS:

- 1. Implement controls to ensure that access to TIMS for employees who have terminated employment is removed in a timely manner.
- 2. Ensure that access to the Customer User Acceptance Team database is limited to authorized users.

SYSTEM ACCESS CONTROLS

E. Number of Log-In Attempts

Condition: OMM's number of unsuccessful log-in attempts to access TIMS exceeded the

standard established by the Department of the Interior. Specifically, TIMS users were allowed six unsuccessful log-in attempts before the user was

locked out of the system.

Criteria: The Department's "Automated Information Systems Security Handbook"

specifies three as the number of unsuccessful log-in attempts.

Cause: OMM information technology officials did not ensure that the number of

allowed unsuccessful log-in attempts was established in accordance with Departmental standards. OMM information officials stated that log-in attempt policies were set using the default settings recommended by the software vendor and the defaults set by the Royalty Management Program. However, security management officials of the Royalty Management Program had requested and were granted a waiver to deviate from the Departmental standard by the Department's Office of Information Resources

Management.

Effect: As a result, the increased number of invalid attempts reduced the

effectiveness of the password as an access control. In addition, the risk was

increased for unauthorized access to sensitive TIMS data.

Recommendation

We recommend that the Director of MMS evaluate the risk involved in deviating from the Department of the Interior standard for the number of unsuccessful log-in attempts. If the Director determines that the number of invalid attempts should remain at six, OMM management should request a waiver from the Department to deviate from the standard of three attempts.

SYSTEM ACCESS CONTROLS

F. Password Management

Condition: The password controls established by OMM in the Windows NT operating

system allowed all system users to retain passwords indefinitely, even though the system required users to change their passwords after 90 days. The controls did not require that a password history be maintained, and the controls allowed users to change their passwords consecutively until the

original password could be reused.

Criteria: The security of a password system is dependent upon keeping passwords

secret. NIST Federal Information Processing Standards Publication 112, "Password Usage," states that passwords "should be changed periodically with a maximum interval selected by the Security Officer." The Publication further states that the system "should check that the new password is not the same as the previous password" or any number of previous passwords and

maintain a history of the passwords of each user.

Cause: OMM information technology officials did not change Windows NT

password default settings to ensure that passwords were not reused or cycled

through quickly.

Effect: As a result, the risk was increased that a password could be discovered and

used to obtain improper access to TIMS.

Recommendation

We recommend that the Director of MMS implement controls to ensure that system software settings are established to prevent users from reusing passwords or cycling through passwords quickly.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

G. Software Change Request and Approval Process

Condition:

At the Gulf of Mexico Region, formal software change control procedures had been developed and implemented for the ongoing support and maintenance of TIMS. However, we found that OMM Information Technology Division personnel did not ensure that change requests were received from authorized users; that the changes were coordinated among all the OMM regions; and that all changes were reviewed, approved, and prioritized by the OMM Maintenance Change Board. During October 1998 through June 1999, there were 1,157 change requests for TIMS, of which we statistically selected 132 changes¹ to determine the adequacy of the change management process. We found that of the 132 sampled change requests, 24 change requests (19 percent) were not submitted by an authorized user representative and 130 change requests (98 percent) were not coordinated with user representatives in the other three OMM regions. We also found no documentation to support that the changes had been reviewed and prioritized by the Maintenance Change Board.

Criteria:

NIST Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," prescribes guidelines for maintaining software. According to the Publication, the primary purpose of change control (or change management) is to ensure smooth operational continuity and orderly evolution of the system. Effective change controls are needed to ensure that all software installations are performed in a structured and controlled manner and provide management with a chronological history of all software modifications. Key change management control points ensure that all changes to hardware and software are formally requested, approved, and documented. In addition, the Publication states that "there should be a centralized approval point for all software maintenance projects." Also, the "TIMS Methodology Handbook" states that Customer User Acceptance Team "leaders in the regions [should] coordinate program changes and issues among themselves before submitting a written request to the Information Technology Division." In addition, the Handbook requires the Maintenance Change Board to review and prioritize software change requests.

Cause:

Division personnel did not enforce OMM policies and procedures that required change requests to be accepted from Customer User Acceptance

¹Although we selected 132 change requests for review, we did not review all of the requests for specific attributes because some of the requests selected were canceled or were not completed at the time of our review.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

Team leaders only, to be coordinated among the OMM regions, and to be reviewed and prioritized.

Effect:

As a result, the risk is increased that operational problems will be introduced into the TIMS production environment. Because change requests result in changes to the TIMS production environment and implemented in all OMM regions, the lack of controlling and coordinating change requests among the Customer User Acceptance Team leaders could result in changes being made for one region that affect another region's ability to access and process transactions efficiently and effectively. Further, the resultant errors and production problems could be time-consuming and difficult to diagnose and correct. Additionally, without reviews and prioritization of change requests, there is little assurance that the most critical changes will be implemented first.

Recommendations

We recommend that the Director of MMS:

- 1. Enforce TIMS change control policies and procedures to ensure that all modifications are properly coordinated, authorized, approved, reviewed, and prioritized.
- 2. Evaluate the current policy for submitting changes to TIMS and determine whether the number of authorized persons who submit software changes can be reduced.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

H. Testing

Condition:

Testing and documentation of software changes to TIMS were not adequate. Specifically, we found that, of the 108 changes tested, 62 changes (57 percent) did not have test plans. In addition, 24 (24 percent) of 100 changes were not tested by either the quality assurance group or the user group (see footnote 1 in Finding G).

Criteria:

Publication 106 states that testing standards and procedures "should define the degree and depth of testing to be performed and the disposition of test materials upon successful completion of the testing." Also, the Publication states that testing is a critical component of software maintenance and that test plans should define the expected output of a test and test for valid, invalid, expected, and unexpected cases. In addition, the "TIMS Methodology Handbook" states that test plans are to be developed and kept current for each of the TIMS components. Test plans also became required documentation in 1998.

Cause:

Although OMM had policies and procedures for software development and change management, OMM management did not ensure that the software change policies and procedures were complied with.

Effect:

As a result, the risk was increased that processing irregularities or malicious codes could be introduced, sensitive data could lack integrity, and TIMS applications may not function to meet user requirements.

Recommendation

We recommend that the Director of MMS enforce its policies and procedures for developing test plans, testing software changes, and documenting test results for all changes made to TIMS.

COMPONENTS OF TECHNICAL INFORMATION MANAGEMENT SYSTEM

Adjudication Tracking System (ATS)

Block and Boundary

Supplemental Bonding

Certs

Civil Penalty

Company and Bonding

Element Data Dictionary

Environmental: Coris

Environmental: Physical

Environmental: Social

Events

Form Navigation

Geologic

Inspections

Lease Administration

Lease Status

Lease Suspensions

Meters

Oil Spill Financial Responsibility

Performance review

Pipelines

Plans

Platforms

Post Sale

Presale

Production

Public Information

Rate Control

Reserves

Rigs

Royalty Relief

Sale

Sampling

Security

Seismic

TIMS Methodology

TIMS Shared

TIMS Support library

Tract Evaluation

Units

Wells



United States Department of the Interior

MINERALS MANAGEMENT SERVICE Washington, DC 20240



JUL 19 2000

Memorandum

To:

Assistant Inspector General for Audits

Sylvia V. Baca

PietdeWit Ju 24 2000

Assistant Secretary, Land and Minerals Management

From:

Walt Rosenbusch Thomas RK1+500, For Director, Minerals Management Service

Subject:

Office of Inspector General Draft Audit Report, "General and Application Controls Over the Technical Information Management System, Offshore Minerals Management, Minerals Management Service" [A-IN-MMS-001-

Thank you for the opportunity to respond to the draft audit report on our Technical Information Management System. We are providing to you our general comments on the audit findings and specific ones on the recommendations. We agree with all 15 recommendations and are in the process of implementing them.

Please contact Bettine Montgomery at (202) 208-3976 if you have any further questions.

Attachment

Minerals Management Service Response to Draft Audit Report "General and Application Controls System"

Audit Agency:

Office of Inspector General

Report Number:

A-IN-MMS-001-99-R (May 2000)

GENERAL COMMENTS

We appreciate the opportunity to review and comment on the Office of Inspector General's draft audit report referenced here. Overall, we believe this was a fair evaluation of the Technical Information Management System in our New Orleans Office. We concur with all the recommendations provided in the report. We will respond to each of the eight weaknesses identified by providing (1) how we have already addressed improving the controls over TIMS, (2) how we plan to address improving the controls that are not currently in place, or (3) information in support of the controls we have in place, and therefore challenge the findings of the OIG.

COMMENTS ON WEAKNESSES AND RECOMMENDATIONS

A. Computer Security Plan: MMS had not developed a security plan for TIMS, which has been identified by MMS as a sensitive and mission critical system.

Recommendation A1. We recommend that the Director of MMS ensure that a computer security plan for TIMS is developed, implemented, and monitored in accordance with the United States Code, Office of Management and Budget Circular A-130, and National Institute of Standards and Technology guidelines.

Response: <u>AGREE</u> – MMS has identified TIMS as a sensitive and mission critical system. Because of this designation, the Offshore Minerals Management Program had a draft security plan that was provided to the OIG Auditor. This plan was in addition to the TIMS Y2K document addressed in the Report. We agree that our plan did not meet the statutory requirements for a security plan. During the audit, OMM began the development of a plan to meet the requirements addressed in OMB Circular A-130, Appendix III, and NIST Special Publication 800-18.

The responsible official is the Chief, Information Technology Division

Target Date: We plan to have a draft document prepared for review by the end of October 2000 and a final computer security plan completed by no later than March 2001. By the time the security plan for TIMS is completed, all OMM users will have been trained on their security responsibilities in the use of the system.

B. Computer Security Training: Mandatory computer security awareness training had not been provided to OMM employees and contractor personnel.

Recommendation B1. Implement policies and procedures to ensure that OMM employees and contractor personnel who are involved with sensitive component systems receive annual computer security awareness training.

Response: AGREE - OMM has not held periodic training as required by the Computer Security Act of 1987 (P.L.100-235) for "all employees [and contractors] who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency." We are in the process of developing and implementing policies and procedures to ensure that employees and contractor personnel receive periodic computer security awareness training. Nowhere in the laws and regulations did we find that the training is mandatory on an annual basis. OMM will provide security awareness training for new employees and contractors within 60 days of working on the OMM systems. All new employees and contractors must complete a Computer Services Access Request form prior to receiving an account on the MMS computer system. This request form includes five security statements that require the user's signature before the account is assigned.

OMM has appointed a new security officer and recently hired a security specialist to develop, implement, and monitor security policy. These individuals also are charged with the development and implementation of a computer security awareness training program for users, systems administrators, and management within OMM. All OMM employees and contractors will participate in a security awareness-training program before the end of Calendar Year 2000. All employees will have, at a minimum, computer awareness training every even numbered calendar year. Periodic security alerts will be sent to all employees on an as needed basis, or as conditions warrant an update.

Recommendation B2. Ensure that training is documented in the employee human resources files.

Response: <u>AGREE</u> - OMM will ensure that the computer security awareness training is documented in the employee's human resources file.

The responsible official is the Deputy Associate Director for Offshore Minerals Management.

Target date: We will train all OMM employees and contractors in computer security awareness by December 2000.

C. Service Continuity: OMM did not have an effective means of recovering or continuing critical TIMS functions and operations in the event of a system failure or a disaster. The Gulf of Mexico Region's April 1996 Continuity of Operations Plan has not been tested. The Plan did not include recovering critical TIMS development and maintenance functions. The Regional personnel responsible for the Plan had not been trained in their roles and responsibilities. The Plan was not available at the designated offsite storage facility. The backup tapes of critical TIMS data and applications were not routinely transferred to the offsite storage facility.

Recommendation C1. Develop a Continuity of Operations Plan for the Offshore Minerals Management Information Technology Division, which includes procedures for recovery of the Division's critical TIMS functions.

Response: AGREE – Since the audit was conducted, OMM has reorganized various functions within the New Orleans Office. We have moved all TIMS server hardware, development, and Gulf of Mexico Region production under one management structure. A new Continuity of Operations Plan has been finalized for the New Orleans computer center that includes all hardware operations at that location. The Plan also includes procedures for the recovery of critical TIMS functions.

Recommendation C2. Periodically test the Continuity of Operations Plan and update the Plan based on the test results.

Response: AGREE – We plan to test the New Orleans Continuity of Operations Plan prior to the end of Calendar Year 2000 and on a regular basis in the future.

Recommendation C3. Ensure that copies of the Continuity of Operations Plan are maintained at the offsite facility.

Response: <u>AGREE</u> – An updated copy of the Continuity of Operations Plan can be found in the Headquarters office of the Information Technology Division and also at a new offsite storage facility in the New Orleans area.

Recommendation C4. Ensure that backup copies of TIMS applications, components, and data are stored at the offsite storage facility on a routine cyclical basis.

Response: <u>AGREE</u> – We have established and implemented new backup procedures. We also store backup copies of the TIMS applications, components, and data at the new offsite storage facility in the New Orleans area. These items are rotated on a routine basis as defined in the Continuity of Operations Plan. All boxes are clearly labeled for quick recovery.

Recommendation C5. Provide training to OMM personnel who are responsible for the recovery of critical TIMS business functions and operations about their roles and responsibilities related to the Continuity of Operations Plan.

Response: AGREE – We will train OMM personnel concerning their roles and responsibilities for the recovery of critical TIMS business functions and operations.

The responsible official is the Regional Director, Gulf of Mexico Region.

Target date: Test New Orleans Continuity of Operations Plan by December 2000.

D. User Access: OMM did not adequately control access to the TIMS databases. Specifically, employees who were no longer employed by MMS still had access to the TIMS.

Recommendation D1. Implement controls to ensure that access to TIMS for employees who have terminated employment is removed in a timely manner.

Response: <u>AGREE</u> -When an employee leaves the Bureau, a procedure is in place to terminate all access to the MMS and TIMS systems.

Recommendation D2. Ensure that access to the Customer User Acceptance Team database is limited to authorized users.

Response: <u>AGREE</u>: - We have implemented new procedures to ensure that access is available only to those who have a need to know the TIMS information. Procedures have also been put in place to provide access to only those who have completed a user access form. The Office of Responsibility must also grant permission prior to the user having access to the TIMS data. We have established a database to track user access to the TIMS system. The same procedures will be followed for all employees requiring access to the Customer User Acceptance Team database.

The responsible official is the Deputy Associate Director, Offshore Minerals Management.

Target date: Task Completed.

E. Number of Log-In Attempts: OMM's number of unsuccessful log-in attempts to access TIMS exceeded the standard established by the Department of the Interior. Specifically, TIMS users were allowed six unsuccessful log-in attempts before the user was locked out of the system.

Recommendation E1. MMS should evaluate the risk involved in deviating from the Department of the Interior standard for the number of unsuccessful log-in attempts. If the Director determines that the number of invalid attempts should remain at six, OMM management should request a waiver from the Department to deviate from the standard of three attempts.

Response: AGREE - The number of unsuccessful log-in attempts has been established at three unsuccessful log-in attempts before the user is locked out of the system.

The responsible official is the Deputy Associate Director, Offshore Minerals Management.

Target Date: Task Completed.

F. Password Management: The password controls established by OMM in the Windows NT operating system allows all system users to retain passwords indefinitely, even though the system required users to change their passwords after 90 days. The controls did not require that a password history be maintained, and the controls allowed users to change their passwords consecutively until the original password could be reused.

Recommendation F1. MMS should implement controls to ensure that system software settings are established to prevent users from reusing passwords or cycling through passwords quickly.

Response: <u>AGREE</u> - All NT servers that are supported by OMM and MMS have the password setting to prevent the reuse or quick recycling of passwords. These passwords must be changed every 90 days. The Council of Information Management Officials established this policy on behalf of the Bureau.

The responsible officials are members of the Council of Information Management Officials.

Target Date: Task Completed.

G. Software Change Request and Approval Process: At the Gulf of Mexico Region, formal software change control procedures had been developed and implemented for the ongoing support and maintenance of TIMS. However, we found that OMM Information Technology Division personnel did not ensure that change requests were received from authorized users; that the changes were coordinated among all the OMM regions; and that all changes were reviewed, approved, and prioritized by the OMM Maintenance Change Board. We also found no documentation to support that the changes had been reviewed and prioritized by the Maintenance Change Board.

Recommendation G1. Enforce TIMS change control policies and procedures to ensure that all modifications are properly coordinated, authorized, approved, reviewed, and prioritized.

Response: <u>AGREE</u>: - The Information Technology Division has not been in the position to reject the TIMS maintenance and/or enhancement change requests submitted by the program office. In the early development of TIMS, OMM established the Component User Acceptance Team leader concept for each major subject area of TIMS to be the focal point for ongoing program changes. The Teams are responsible for the program view and coordination of their respective components. The Information Technology Division implemented the change requests as submitted.

To deal with the large number of change requests, the TIMS Project Office established a Change Control Group (called Maintenance Change Board in the Report). The Information Technology analyst who knew the design and was responsible for the maintenance of the TIMS components was a member of this Group. The TIMS Maintenance Methodology states that all requests will be reviewed and prioritized, and deadlines will be set for implementation. All change requests are entered into the tracking system called Defect Control System. The Change Control Group reviewed all outstanding work requests in the Defect Control System and made assignments to the staff, weekly. The tracking of the request in the Defect Control System was the documentation.

The OMM Information Technology Division staff did not track nor collect information in reference to the Component User Acceptance Team coordinating change requests with peers in other regions. That is the responsibility of the Team leader. Upon completion of a work

request of the Information Technology Division staff, all Component User Acceptance Teams for that component were notified by the Information Technology Division that the work request was completed. The module was then ready for testing prior to final deployment to all OMM sites.

In October 1999, the Information Management Committee determined that it needed to better manage the change control policies and procedures. The Committee authorized the creation of a new TIMS Change Control Board. The Board is comprised of representatives from the OMM program offices and Chaired by the Deputy Regional Director of the Gulf of Mexico Region. The purpose of the Change Control Board is to review, monitor, evaluate, approve/disapprove, and prioritize all enhancement and maintenance requests (submitted by the TIMS users) for current TIMS components. The Board will also review usage of the TIMS forms and reports and eliminate unused or underutilized and non-critical forms and reports.

With the development of this Board, all programmatic changes, corrections, amendments, reforms, improvements, enhancements, or upgrades made to the TIMS components are reviewed, approved/disapproved, and prioritized. This review also entails an evaluation of the potential costs and benefits of proposed changes.

Recommendation G2. Evaluate the current policy for submitting changes to TIMS and determine whether the number of authorized persons who submit software changes can be reduced.

Response: <u>AGREE</u> - The Change Control Board is not only responsible for enforcing the change control policies and procedures, but also controls the number of changes that can be made to the system. The Information Technology Division is in the final stage of implementing a replacement for the work request tracking system known as Defect Control System. The new software system is a commercial off-the-shelf solution called Visual Interceptor. Interceptor is web based and will only allow authorized Component User Acceptance Teams to forward approved work requests to the Change Control Board for final review and prioritization. This new web-based system will be in place by the end of calendar year 2000.

The responsible official is the Deputy Associate Director for Offshore Minerals Management.

Target Date: Policy to limit number of persons submitting changes – Completed.

Implementation of request tracking by December 2000.

H. Testing: Testing and documentation of software changes to TIMS were not adequate. Specifically, we found that, of the 108 changes tested, 62 changes (57 percent) did not have test plans. In addition, either the quality assurance group or the user group did not test 24 of 100 (24 percent) changes.

Recommendation H1. MMS should enforce its policies and procedures for developing test plans, testing software changes, and documenting test results for all changes made to TIMS.

Response: AGREE – We agree with the recommendation made in the report that OMM should enforce the TIMS Maintenance Methodology policies and procedures related to testing and its documentation. We do not agree with the analysis that drew the auditors to their recommendations. Based on our analysis of the full 132 sample set, our findings are different from the auditor. Specifically, of the 62 changes (57 percent) that did not have individual test plans, OMM determined 59 changes to be exceptions that did not require test plans. Although the TIMS Maintenance Methodology requires test plans, there are certain changes that are considered routine and/or minor and, therefore, would not require individual test plans. These exceptions include reports (41); and system administration functions, database triggers, packages, and menu change requests (18). Therefore, OMM found that only 3 of the 62 changes should have had test plans based on the TIMS Maintenance Methodology. Reports are covered by a generic test plan since they are fairly simple and do not require individual test plans.

In addition, we concur that the quality assurance or the user group did not test 24 of 100 changes. We determined that there were 20 exceptions to these changes. These exceptions included data dictionary, domain value, or menu changes. The Database Administrator makes these changes and, upon completion, the Component User Acceptance Team members or an analyst tests the change. We conclude that there were only four changes that were not tested before they were put on the production machine. Therefore, the quality assurance group or the user group did not test only 4 percent of the changes.

The Information Technology Division is converting to a new change control tracking system, called Visual Interceptor, that will better serve our customers with online web access to the status of all change requests. We will properly identify all stages of the life cycle of a change request. This new system should be fully operational by the end of the calendar year 2000. A change request can be submitted for many Information Technology functions, not just a change to a TIMS program.

We recognize the need for test plans and for adequate testing of the changes, and we plan to continue this process. We also have tightened up and enforced the policies and procedures we have in place. There are numerous exceptions and alternative test procedures that accompany the change management. These exceptions need to be further identified in our TIMS Maintenance Methodology. We will continue our review of existing methodology to expand testing and acceptance criteria to improve the process. Documentation will occur through the implementation of the new change control tracking system.

The responsible official is the Deputy Associate Director for Offshore Minerals Management.

Target Date: Enforcement of required test plans and testing – Completed.

Implementation of request tracking by December 2000.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Actions Required
A.1, B.1, B.2, C.2, C.5, G.2, and H.1	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
C.1, C.3, C.4, D.1, D.2, E.1, F.1, and G.1	Implemented.	No further response is required.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL

Internet Complaint Form Address

http://www.oig.doi.gov/hotline form.html

Within the Continental United States

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 - MIB Washington, D.C. 20240-0001 Our 24-hour Telephone HOTLINE 1-800-424-5081 or (202) 208-5300

TDD for hearing impaired (202) 208-2420

Outside the Continental United States

Caribbean Region

U.S. Department of the Interior Office of Inspector General Eastern Division - Investigations 4040 Fairfax Drive Suite 303 Arlington, Virginia 22203 (703) 235-9221

Pacific Region

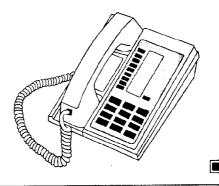
U.S. Department of the Interior Office of Inspector General Guam Field Pacific Office 415 Chalan San Antonio Baltej Pavilion, Suite 306 Agana, Guam 96911 (671) 647-6060

HOTLINE

U.S. Department of the Interior Office of Inspector General 1849 C Street, NW Mail Stop 5341- MIB Washington, D.C. 20240-0001

Toll Free Number 1-800-424-5081

Commercial Numbers (202) 208-5300 TDD (202) 208-2420





U.S. Department of the Interior Office of Inspector General

REPORT

DEPARTMENT OF THE INTERIOR ACTIVITIES
TO COLLECT, REVIEW, AND USE
INFORMATION THAT IDENTIFIES
INDIVIDUALS WHO ACCESS THE
DEPARTMENT'S INTERNET SITES

REPORT NO. 01-I-340 APRIL 2001



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

April 30, 2001

Memorandum

To:

Chief Information Officer, Department of the Interior

From:

Roger La Rouche

Assistant Inspector General or Audits

Subject: Report on Department of the Interior Activities To Collect, Review, and Use Information That Identifies Individuals Who Access the Department's Internet

Sites (Report No. 01-I-340)

Provided for your information is a copy of the Office of Inspector General's report (Attachment) on the Department of the Interior's (DOI) activities to collect, review, and use information that identifies individuals who access the Department's Internet sites. This report will be provided to the Congress as required by Section 646 of the Treasury and General Appropriations Act, 2001.

We found that generally the DOI and its components and third parties did not collect, review, or obtain singular data or create aggregate lists that included personally identifiable information about individuals who accessed the DOI Web pages. Additionally, we found that generally the DOI notified users when personally identifiable information was being collected and explained their use of this information. However, we found some exceptions in the 598 Web pages reviewed. These exceptions were as follows:

- "Cookies" were not disclosed to the Internet users on 29 Web pages.
- Web bugs existed on 12 Web pages.
- Of the 84 Web pages that collected personally identifiable information, 17 did not disclose to the Internet user all uses of this information.
- Of the five third-party contractors that collected personally identifiable information, three did not disclose all uses of the collected information.

We shared with the agencies' Web masters the results of our review. In most cases, the Web masters began taking corrective actions.

If you have any questions concerning this report, please contact me at (202) 208-4252 or Ms. Diann Sandy, Director of National Information Systems Office, at (303) 236-9243.

Attachment

cc: Assistant Secretary for Policy, Management and Budget

Assistant Secretary for Fish and Wildlife and Parks

Assistant Secretary for Indian Affairs

Assistant Secretary for Land and Minerals Management

Assistant Secretary for Water and Science

Director, Bureau of Land Management

Commissioner, Bureau of Reclamation

Director, Minerals Management Service

Director, National Park Service

Director, Office of Surface Mining Reclamation and Enforcement

Director, U. S. Fish and Wildlife Service

Director, U.S. Geological Survey

Audit Liaison Officer, Policy, Management and Budget

Audit Liaison Officer, Fish and Wildlife and Parks

Audit Liaison Officer, Indian Affairs

Audit Liaison Officer, Land and Minerals Management

Audit Liaison Officer, Water and Science

Audit Liaison Officer, Bureau of Land Management

Audit Liaison Officer, Bureau of Reclamation

Audit Liaison Officer, Minerals Management Service

Audit Liaison Officer, National Park Service

Audit Liaison Officer, Office of Surface Mining Reclamation and Enforcement

Audit Liaison Officer, U.S. Fish and Wildlife Service

Audit Liaison Officer, U.S. Geological Survey

REPORT ON

DEPARTMENT OF THE INTERIOR ACTIVITIES TO COLLECT, REVIEW, AND USE INFORMATION THAT IDENTIFIES INDIVIDUALS WHO ACCESS THE DEPARTMENT'S INTERNET SITES

As required by Section 646 of the Treasury and General Appropriations Act, 2001, we reviewed the Department of the Interior's (DOI) Web pages to identify the DOI's activities related to:

- Collecting or reviewing singular data or creating aggregate lists that include personally identifiable information about individuals who access any Internet site¹ of the DOI.
- Entering into agreements with third parties, including other government agencies, to collect, review, or obtain aggregate lists or singular data containing personally identifiable information relating to any individual's access or viewing habits of governmental and nongovernmental Internet sites.

RESULTS OF REVIEW

The DOI generally did not inappropriately collect personally identifiable information on individuals who accessed its

Internet Web pages. Of the DOI's more than 6,000 Web pages, we reviewed 598, including the DOI's 532 Internet sites. We found that generally the DOI and its components and third parties did not collect, review, or obtain singular data or create aggregate lists that included personally identifiable information about individuals who accessed the DOI's Web pages. Additionally, we found that generally the DOI notified users when personally identifiable information was being collected and explained its use of this information. However, we found some exceptions in the Web pages reviewed. These exceptions were as follows:

- "Cookies" were not disclosed to the Internet user on 29 Web pages.
- Web bugs existed on 12 Web pages.
- Of the 84 Web pages that collected personally identifiable information, 17 did not disclose to the Internet user all uses of this information.

¹An Internet site is defined as an agency's principal Web pages; other major entry points to sites, including home pages of agency components and Web pages that receive a high number of visits; and any Web page where substantial amounts of personal information are collected or posted.

 Of the five third-party contractors that collected personally identifiable information, three did not disclose all uses of the collected information.

The details of our review are discussed in the paragraphs that follow.

"COOKIES" AND WEB BUGS

Session or Persistent "Cookies" Used and Not Disclosed We found that of the 598 Web pages reviewed, 17 had session "cookies" (see Appendix 1). Of these 17 Web pages, only 4 disclosed the use of session "cookies." We also found 18 Web pages that had persistent

"cookies" (see Appendix 2). Of these 18 Web pages, 16 did not disclose to the Internet user that persistent cookies were being used. In addition, agency head approvals for these 18 Web pages were not provided to us. Rather than providing us with agency head approvals, the Web masters removed the persistent "cookies" from nine of the Web pages, and three Web pages could no longer be accessed. We verified that as of April 17, 2001, these 12 persistent "cookies" no longer existed or the Web pages could not be accessed. For the remaining six Web pages, we found that as of April 17, 2001:

- One Web page had been updated to disclose the use of a persistent "cookie."
- Five Web pages continued to use persistent "cookies" without disclosure of their use.
- None of the six Web pages had agency head approval for the use of "cookies."

We also followed up on the General Accounting Office's report "Internet Privacy: Federal Agency Use of Cookies," issued in October 2000. In that report, the General Accounting Office identified two DOI Web sites that included session "cookies" (www.blm.gov and reservations.nps.gov) that were not disclosed. As of April 17, 2001, we found that www.blm.gov no longer had a session "cookie" but that reservations.nps.gov continued to have a session "cookie" and the use of the session "cookie" was not disclosed. National Park Service (NPS) management is addressing this issue.

2

²A "cookie" is a mechanism that the Web server uses to store a small piece of information on the client's (user's) computer. A session cookie is stored on the user's computer only during the browsing session. A persistent cookie is stored on the user's computer during the browsing session and remains after the session is closed.

Web Bugs Were Detected

We found that 12 of the 598 Web pages contained a Web bug³ (see Appendix 3). Further, the use of the Web bug was not disclosed on the Web page privacy notice.

We contacted Chief Information Officer management and Web masters regarding the use of Web bugs. In four of the cases, the Web bugs were removed. We verified that as of April 17, 2001, the four Web bugs no longer existed on these Web pages. In none of the 12 instances were we provided information to support the use of the Web bug.

COLLECTING PERSONALLY IDENTIFIABLE INFORMATION

Personally Identifiable Information Collected and Not Always Disclosed Our audit staff, with the assistance of the DOI and its components, identified that at least 84 of the 598 Web pages collected personally identifiable information. We reviewed these 84 Web pages and found that 62 contained disclosures related to the use of the personally

identifiable information collected and 5 could not be accessed. Additionally, the privacy notice statements on these 62 Web pages indicated that the personally identifiable information collected was subject to disclosure but would be handled in accordance with the requirements of the Privacy Act and the Freedom of Information Act to ensure the greatest protection of personal privacy in the event of any required disclosure. The privacy notice further stated that unless required by law, the personally identifiable information would not be shared with outside parties.

Of the 17 Web pages that collected personally identifiable information and this fact was not disclosed, we found that 10 were for users to submit comments or feedback to the agency. Personally identifiable information was collected only if the user requested a response. Generally, the personally identifiable information collected included the Internet users' name, home address, and electronic mailing address. The remaining seven Web pages were for users to perform such actions as submitting applications for positions, registering for conferences, and downloading application software.

Personally Identifiable Information Collected and Disclosed When Submitting Questions Electronically Generally, Internet users that contact the DOI and its components electronically through Web pages to do activities such as to ask questions, provide feedback, fill out questionnaires, or sign guest books provided personally identifiable information

³A Web bug is a mechanism to store a small piece of information on the client computer that can be shared with other sites. In the case of DOI, the Web bugs were third-party cookies stored on the client computer by a software vendor and not the host of the Web page.

⁴ These Web pages do not include Web sites addressed under the "Third Parties Collecting Personally Identifiable Information" section of this report.

voluntarily. Of the 598 Web pages, 310 included privacy notice statements. If the Internet user wanted to contact the agency through a Web page, the DOI's privacy notice statements disclose the use of any personally identifiable information collected. Further, these privacy notices provide the user assurance that the personally identifiable information collected when contacting the DOI or its components will not be shared with any entity outside the DOI. Although the remaining 288 Web pages reviewed did not contain privacy notice statements, these pages generally were not used to contact the agency to ask questions (see Appendix 4).

THIRD PARTIES COLLECTING PERSONALLY IDENTIFIABLE INFORMATION

We reviewed five Web pages that were maintained by third-party organizations for the DOI. These Web pages were generally for the purposes of transacting business with the Internet user. The following were the specific purposes of these five Web pages:

- Purchasing Federal Duck Stamps
- Obtaining geological reference materials
- Adopting a wild horse or burro
- Making a reservation at a national park
- Purchasing a national park pass

All of these Web pages were able to collect Internet users' viewing habits and collect the users' personally identifiable information. Additionally, not all of these Web pages contained privacy statement notices. Specific details of these Web pages are discussed in the paragraphs that follow.

Personally Identifiable Information Collected and Not Disclosed When Purchasing a Federal Duck Stamp We were provided a copy of the agreement between the U.S. Fish and Wildlife Service and its contractor that sold Federal Duck Stamps. The contract did not address the collection and/or distribution of the personally identifiable information. Further, the contractor's Web pages did not contain a

privacy statement that disclosed the use of the personally identifiable information collected to purchase a Federal Duck Stamp or that stated whether aggregate lists of viewing habits were shared or otherwise disclosed to other parties. Additionally, for the Internet user to purchase a Federal Duck Stamp, substantial personally identifiable information was needed, including a credit card number. When we contacted contractor personnel, they stated that the buyer information was not shared.

Personally Identifiable Information Collected for Geological References May Be Shared We received a copy of the agreement between the U.S. Geological Survey and its geological reference material contractor. The contractor's Web page did include a privacy statement that indicated information may be shared. When discussed with Geological Survey Information Technology management, they said that the reference to the Federal Acquisition Regulation clauses in the agreement prohibited the contractor from disclosing or otherwise sharing the personally identifiable information and the Internet users' aggregate viewing habits that could be collected. In our review of the Federal Acquisition Regulation clauses included in the agreement, we did not find a reference that the contractor was prohibited from sharing or disclosing personally identifiable information and the Internet users' viewing habits.

Personally Identifiable Information Collected but Not Disclosed When Adopting a Wild Horse or Burro The Web pages maintained by a contractor for adopting a wild horse or burro did not contain adequate privacy information regarding the use and disclosure of the personally identifiable information collected from the Internet user. This is of concern because two of the Web pages we reviewed contained a

Web bug that was a third-party software provider "cookie" and could be used to share the Internet users' viewing habits. Further, although we requested a copy of the agreement, we had not received a copy by the time we prepared our report. The Web page where personally identifiable information was collected required the applicants to provide the following:

- Name, address, telephone number, and electronic mailing address.
- Driver's license number.
- Social security number.

We requested additional information regarding the use and disclosure of the personally identifiable information collected. As of April 17, 2001, no response had been received.

Personally Identifiable Information Shared With Outside Parties and Not Disclosed When Making a Reservation at a National Park Within the NPS's reservation Web pages that are maintained and operated by a contractor, we found that when making a reservation at Mammoth Cave the Internet users' personally identifiable information could be shared with outside parties. Further, the Web page did not explicitly state that the users' personally identifiable information may be shared with a

party outside of the NPS and its contractor. The NPS and its contractor stated that the users' personally identifiable information would be provided to the other third party only if the users acknowledged that they wanted additional information about the Mammoth Cave area. We received a copy of the agreement between the NPS and the organization that received the personally identifiable information. The NPS has modified the contract to make it explicit that once the user has been provided the information about Mammoth Cave, the personally identifiable information collected will be destroyed.

However, the Web page privacy notice was not modified to inform the Internet users that their personally identifiable information may be shared.

Internet Users' Viewing Habits Shared When Purchasing a National Park Pass The NPS contractor collected personally identifiable information when an Internet user purchased a national park pass. The contractormaintained Web site included a privacy notice statement that disclosed that

Internet users' viewing habits, in aggregate, may be shared for research purposes with whomever the contractor chooses. The NPS policy is to notify Internet users whenever the user leaves the NPS Web page to visit a third party's Web page unless the site has been reviewed and approved by formal agreement. When Internet users accessed the Web page to purchase a park pass, the users were not warned that they were leaving the NPS Web page and accessing a third-party Web page. We were not provided the agreement between the NPS and its contractor for managing the purchase of passes to national parks by the time we prepared our report. Without the opportunity to review this formal agreement, we were not able to determine whether the contractor had been authorized by the NPS to share the Internet users' personally identifiable information or viewing habits with others.

SCOPE AND METHODOLOGY

We reviewed Web pages that were identified as major or principal entry points by the DOI Web masters. In addition, we randomly selected other DOI Web pages and Web pages or sites maintained by third parties. The Web pages selected for the review were those in existence as of February 1, 2001. We used an optional feature offered by the Microsoft browser to identify the use of "cookies" and used Web bug detection software recommended by the General Accounting Office. If we found evidence of the use of session or persistent "cookies," we reviewed the Web page for proper disclosure information and requested proof of the agency head's approval for the use of persistent "cookies."

This review was conducted in accordance with guidance provided by the President's Council on Integrity and Efficiency, issued specifically for this review. Fieldwork was performed during January through April 2001 at the Web master offices in Washington, D.C., and our office in Denver, Colorado.

Department of the Interior Web Pages Reviewed That Used Session Cookies

Bureau	Web Page Address	Status as of April 17, 2001
BLM	http://www.adoptahorse.blm.gov	Session cookie disclosed
BLM	http://www.adoptahorse.blm.gov/adopt- app.asp	Session cookie disclosed
BLM	http://www.glorecords.blm.gov/	No change
BLM	http://www.id.blm.gov/	Session cookie disclosed
DOI	http://www.doi.gov/non-profit/pppx.html	No change
MMS	http://www.gomr.mms.gov/homepg/fastfacts/api/master.asp	No change
MMS	http://www.mms.gov/query.asp	No change
NPS	http://reservations.nps.gov/	No change
USGS	http://earthexplorer.cr.usgs.gov/	Session cookie disclosed
USGS	http://earthexplorer.usgs.gov/	No change
USGS	http://edcnts11.cr.usgs.gov/metalite/ feedback.asp	No change
USGS	http://edcsnw3.cr.usgs.gov/igdn/igdn.html	No change
USGS	http://interactive.usgs.gov/eft/logon.asp	No change
USGS	http://mitchnts1.cr.usgs.gov/	No change
USGS	http://ncgmpnt.er.usgs.gov/thematic/	No change
USGS	http://ratbert.wr.usgs.gov/products/ personnel.asp	No change
USGS	http://ratbert.wr.usgs.gov/products/ personnel.aspy	No change

Department of the Interior Web Pages Reviewed That Used Persistent Cookies

Bureau	Web Page Address	Status as of April 17, 2001
BLM	http://nmreports.nm.blm.gov	Could not access site
BLM	http://paria.az.blm.gov	No change
BLM	http://www.ak.blm.gov/emplymnt.html	Persistent cookie removed
DOI	http://www.doi.gov/non-profit odx.html	No change
FWS	http://search.fws.gov	Persistent cookie removed
FWS	http://www.nfws.org	Persistent cookie removed
FWS	http://www.r6.fws.gov/btprairiedog/	Persistent cookie removed
NBC	http://nbc-heat.nbc.gov/	No change - pending approval
NBC	http://www.nbc.gov	Persistent cookie removed
NPS	http://www.nationalparks.org/	Site updated with disclosure of persistent cookie
NPS	http://www.nps.gov/npf/corporate/Tl.htm	Page removed
OSMRE	https://ismdfmnt5.osmre.gov/osm1/login.cfm	No change
USGS	http://kaibab.wr.usgs.gov/	No change
USGS	http://pubs.usgs.gov	Persistent cookie removed
USGS	http://search.usgs.gov	Persistent cookie removed
USGS	http://volcanoes.usgs.gov	Persistent cookie removed
USGS	http://water.usgs.gov	Persistent cookie removed
USGS	http://edcw2ks15.cr.usgs.gov/	No change

Department of the Interior Web Pages Reviewed That Had A Web Bug

Bureau	Web Page Address	Status as of April 17, 2001
BLM	http://www.adoptahorse.blm.gov	No change
BLM	http://www.adoptahorse.blm.gov/adopt- app.asp	No change
BLM	http://www.ntc.blm.gov/	No change
BOR	http://www.lc.usbr.gov/	No change
DOI	http://elips.doi.gov/	Web bug removed
NPS	http://165.83.219.72/hafe/bookshop/index.cfm	Web bug removed
NPS	http://www.nps.gov/npf/corporate/Tl.htm	Page removed
USGS	http://biology.usgs.gov	Web bug removed
USGS	http://biology.usgs.gov/wfrc	No change
USGS	http://fresc.fsl.orst.edu/	No change
USGS	http://vineyard.er.usgs.gov/	No change
USGS	http://www.usgs.nau.edu/staff/	Web bug removed

Department of the Interior Web Pages Reviewed That Did Not Include A Privacy Statement

Bureau	Web Page Address	Status as of April 17, 2001
BIA	http://www.doi.gov/bia/aberdeen	No change
BIA	http://www.doi.gov/bia/ack_res.html	No change
BIA	http://www.doi.gov/bia/aitoday	No change
BIA	http://www.doi.gov/bia/ancestry	No change
BIA	http://www.doi.gov/bia/ancestry.html	No change
BIA	http://www.doi.gov/bia/areas	No change
BIA	http://www.doi.gov/bia/as-ia	No change
BIA	http://www.doi.gov/bia/bar	No change
BIA	http://www.doi.gov/bia/budget	No change
BIA	http://www.doi.gov/bia/ecodev	No change
BIA	http://www.doi.gov/bia/employment	No change
BIA	http://www.doi.gov/bia/gaming	No change
BIA	http://www.doi.gov/bia/information	No change
BIA	http://www.doi.gov/bia/news	No change
BIA	http://www.doi.gov/bia/non_profit/self-gov.html	No change
BIA	http://www.doi.gov/bia/ots	No change
BIA	http://www.doi.gov/bia/realty	No change
BIA	http://www.doi.gov/bia/self-determ	No change
BIA	http://www.doi.gov/bia/tribegovserv	No change
BIA	http://www.doi.gov/bia/tribes	No change
BIA	http://www.doi.gov/bia/tservices	No change
BLM	http://azwww.az.blm.gov/rec.htm	No change
BLM	http://www.adoptahorse.blm.gov/adopt-app.asp	No change
BLM	http://www.ntc.blm.gov/courses/courses.html	No change
BLM	http://www2.az.blm.gov/	No change
BOR	http://www.usbr.gov/non_profit.html#Partnerships	No change
BOR	http://www.usbr.gov/water/coop.html	No change
DOI	http://cdserver.er.usgs.gov/	No change
DOI	http://elips.doi.gov/	No change
DOI	http://momentum.ios.doi.gov/email/doi.cfm	No change
DOI	http://safetynet.smis.doi.gov/	No change

Bureau	Web Page Address	Status as of April 17, 2001
DOI	http://www.doi.gov/budget/	No change
DOI	http://www.doi.gov/cgi-bin/swish/search.pl	No change
DOI	http://www.doi.gov/core/core.htm	No change
DOI	http://www.doi.gov/doi_plw.html	No change
DOI	http://www.doi.gov/febtc/	No change
DOI	http://www.doi.gov/gpra/	No change
DOI	http://www.doi.gov/gpra/stratpln.html	No change
DOI	http://www.doi.gov/htm/doijobs.html	No change
DOI	http://www.doi.gov/htm/pmanager/	No change
DOI	http://www.doi.gov/intl/	No change
DOI	http://www.doi.gov/non-profit odx.html	No change
DOI	http://www.doi.gov/non-profit/edx.html	No change
DOI	http://www.doi.gov/non-profit/fax.html	No change
DOI	http://www.doi.gov/non-profit/index.html	No change
DOI	http://www.doi.gov/non-profit/lawx.html	No change
DOI	http://www.doi.gov/non-profit/nfax.htm.	No change
DOI	http://www.doi.gov/non-profit/pppx.html	No change
DOI	http://www.doi.gov/non-profit/volx.html	No change
DOI	http://www.doi.gov/nrl/	No change
DOI	http://www.doi.gov/oait/links.htm	No change
DOI	http://www.doi.gov/oha/adr/adr2/htm	No change
DOI	http://www.doi.gov/oha/indexdec/htm	No change
DOI	http://www.doi.gov/oirm/records/	No change
DOI	http://www.doi.gov/onepage.htm	No change
DOI	http://www.epa.gov/OWOW/heritage/rivers.html	No change
DOI	http://www.smis.doi.gov/	No change
FWS	http://duckstamps.fws.gov	No change
FWS	http://ecos.fws.gov/webpage/webpage_vip_ listed.html?&code=V&listings=0#A	No change
FWS	http://search.fws.gov	No change
FWS	http://www.fws.gov/r9estaff/newspdg.html	No change
FWS	http://www.r6.fws.gov/pfw/r6pfw4.htm	No change
FWS	http://www.r6.fws.gov/pfw/wy/wy5.htm	No change
FWS	http://www.duckstamp.com	No change

Bureau	Web Page Address	Status as of April 17, 2001
FWS	http://www.nfws.org	No change
FWS	http://www.r6.fws.gov/btprairiedog/	No change
MMS	http://www.gomr.mms.gov/homepg/offshore/ offshore.html	No change
MMS	http://www.gomr.mms.gov/scripts/fastq.htm	No change
MMS	http://www.mms.gov/navbar.htm	No change
MMS	http://www.mms.gov/query.asp	No change
MMS	http://www.mms.gov/search.htm	No change
NBC	http://nbc-heat.nbc.gov/	No change
NBC	http://ideasec.nbc.gov	No change
NBC	http://ideasec.nbc.gov/vendorsearch	No change
NBC	http://www.doi.gov/pam	No change
NPS	http://www.nps.gov/alcatraz	No change
NPS	http://165.83.219.72/hafe/bookshop/index.cfm	No change
NPS	http://www.nps.gov/interp/pksmart.htm	No change
NPS	http://www.nps.gov/npf/corporate/Tl.htm	Page removed
NPS	http://www.nps.gov/pub_att/pressrm.htm	No change
NPS	http://www1.nature.nps.gov/sindex.htm	No change
OSMRE	http://www.osmre.gov/index2.htm	No change
OSMRE	http://www.osmre.gov/links.htm	No change
OSMRE	http://www.osmre.gov/oc1.htm	No change
OSMRE	http://www.osmre.gov/ocnews.htm	No change
OSMRE	http://www.osmre.gov/osmaml.htm	No change
OSMRE	http://www.osmre.gov/osmreg.htm	No change
OSMRE	http://www.osmre.gov/search.htm	No change
OSMRE	http://www.osmre.gov/statisti.htm	No change
OSMRE	https://ismdfmnt5.osmre.gov/osm1/login.cfm	No change
USGS	http://access.usgs.gov/	No change
USGS	http://agdc.usgs.gov/	No change
USGS	http://ak.water.usgs.gov/	No change
USGS	http://ak.water.usgs.gov/Welcome/	No change
USGS	http://ak.water.usgs.gov/Welcome/employees.htm	No change
USGS	http://ardf.wr.usgs.gov/	No change
USGS	http://aslwww.cr.usgs.gov/	No change

Bureau	Web Page Address	Status as of April 17, 2001
USGS	http://bard.wr.usgs.gov/	No change
USGS	http://biology.usgs.gov/wfrc	No change
USGS	http://biology.usgs.gov/wfrc/crrlhome/crrlhome.html	No change
USGS	http://biology.usgs.gov/wfrc/crrlhome/staff.html	No change
USGS	http://biology.usgs.gov/wfrc/ia.htm	No change
USGS	http://biology.usgs.gov/wfrc/profiles.htm	No change
USGS	http://capp.water.usgs.gov/	No change
USGS	http://chht-ntsrv.er.usgs.gov/	No change
USGS	http://cindi.usgs.gov/	No change
USGS	http://clearinghouse4.fgdc.gov/	No change
USGS	http://coast-enviro.er.usgs.gov/	No change
USGS	http://coralreef.gov/	No change
USGS	http://crusty.er.usgs.gov/	No change
USGS	http://ct.water.usgs.gov/	No change
USGS	http://earthexplorer.cr.usgs.gov/	No change
USGS	http://edc.usgs.ceos.org/ceos.html	No change
USGS	http://edc.usgs.gov/programs/NSLRSDA.html	No change
USGS	http://edc.usgs.gov/srord-link.html	No change
USGS	http://edc.usgs.gov/tour/welcome.html	No change
USGS	http://edcdaac.usgs.gov/	No change
USGS	http://edcdgs9.cr.usgs.gov/	No change
USGS	http://edcintl.cr.usgs.gov/adds/adds.html	No change
USGS	http://edcnts11.cr.usgs.gov/	No change
USGS	http://edcnts11.cr.usgs.gov/metalite/feedback.asp	No change
USGS	http://edcnts12.cr.usgs.gov/ned/	No change
USGS	http://edcnts2.cr.usgs.gov/	No change
USGS	http://edcnts9.cr.usgs.gov/	No change
USGS	http://edcsns15.cr.usgs.gov/	No change
USGS	http://edcsns16.cr.usgs.gov/	No change
USGS	http://edcsnw3.cr.usgs.gov/	No change
USGS	http://edcsnw3.cr.usgs.gov/gha/gha.html	No change
USGS	http://edcsnw3.cr.usgs.gov/igdn/igdn.html	No change
USGS	http://edcsnw4.cr.usgs.gov/	No change

Bureau	Web Page Address	Status as of April 17, 2001
USGS	http://edcwww.cr.usgs.gov/earthshots/ slow/tableofcontents	No change
USGS	http://edcwww.cr.usgs.gov/l7dhf/	No change
USGS	http://energy.cr.usgs.gov/	No change
USGS	http://energy.cr.usgs.gov/lillis/	No change
USGS	http://energy.cr.usgs.gov/radon/	No change
USGS	http://energy.er.usgs.gov/	No change
USGS	http://energy.usgs.gov/west.html	No change
USGS	http://erp-web.er.usgs.gov/	No change
USGS	http://fresc.fsl.orst.edu/	No change
USGS	http://fresc.fsl.orst.edu/contact/contact.htm	No change
USGS	http://fresc.fsl.orst.edu/Crater_Project/crater.htm	No change
USGS	http://fresc.fsl.orst.edu/fffacts/moths/moths.htm	No change
USGS	http://fresc.fsl.orst.edu/fffacts/willowfly/wifl_index.htm	No change
USGS	http://fresc.fsl.orst.edu/field_stations/canyonlands/index.html	No change
USGS	http://fresc.fsl.orst.edu/field_stations/olympic/index.html	No change
USGS	http://fresc.fsl.orst.edu/metadata/metadata.htm	No change
USGS	http://fresc.fsl.orst.edu/moss_project/index.htm	No change
USGS	http://fresc.fsl.orst.edu/online/online_docs/amphibians.pdf	No change
USGS	http://fresc.fsl.orst.edu/textonly/contact/contact.htm	No change
USGS	http://fresc.fsl.orst.edu/textonly/metadata/metadata.htm	No change
USGS	http://fresc.fsl.orst.edu/zooplankton/zooindex.htm	No change
USGS	http://ga.water.usgs.gov/	No change
USGS	http://geology.wr.usgs.gov/docs/geologic/ Fort.Irwin.ES.web/Fort.Irwin.html	No change
USGS	http://geology.wr.usgs.gov/gump/	No change
USGS	http://geology.wr.usgs.gov/MojaveEco/	No change
USGS	http://geology.wr.usgs.gov/wgmt/	No change
USGS	http://geology.wr.usgs.gov/wgmt/lasvegas/lvmap.html	No change
USGS	http://geology.wr.usgs.gov/wgmt/ nationalparks/NatParks.html	No change
USGS	http://geology.wr.usgs.gov/wgmt/ncaltransect/nctmap.html	No change
USGS	http://geology.wr.usgs.gov/wgmt/pacnw/pnwmap.html	No change
USGS	http://geomac.usgs.gov/	No change

Bureau	Web Page Address	Status as of April 17, 2001
USGS	http://geomag.usgs.gov/	No change
USGS	http://geonotes.wr.usgs.gov/hazardconf/regform.html	No change
USGS	http://gisdata.usgs.gov/	No change
USGS	http://grid.cr.usgs.gov/	No change
USGS	http://hvo.wr.usgs.gov/earthquakes/felt/	No change
USGS	http://hvo.wr.usgs.gov/earthquakes/felt/reportform.html	No change
USGS	http://il.water.usgs.gov/	No change
USGS	http://infolink.cr.usgs.gov/	No change
USGS	http://interactive.usgs.gov/eft/logon.asp	No change
USGS	http://landsat7.usgs.gov/software/formias.html	No change
USGS	http://landsat7.usgs.gov/software/formlps.html	No change
USGS	http://landslides.usgs.gov/	No change
USGS	http://ma.water.usgs.gov/	No change
USGS	http://mapping-ak.wr.usgs.gov/research.html	No change
USGS	http://mi.water.usgs.gov/	No change
USGS	http://minerals.usgs.gov/west/menlo.html	No change
USGS	http://minerals.usgs.gov/west/notablepeople.html	No change
USGS	http://minerals.usgs.gov/west/people.html	No change
USGS	http://minerals.usgs.gov/west/projectlisting.html	No change
USGS	http://minerals.usgs.gov/west/spokane.html	No change
USGS	http://minerals.usgs.gov/west/tucson.html	No change
USGS	http://mitchnts1.cr.usgs.gov/	No change
USGS	http://motion.wr.usgs.gov/	No change
USGS	http://narl.er.usgs.gov/	No change
USGS	http://nationalatlas.gov/survey/	No change
USGS	http://ncgmp.cr.usgs.gov/ncgmp/lvuc/lvuc.htm	No change
USGS	http://ncgmp.usgs.gov/	No change
USGS	http://ncgmpnt.er.usgs.gov/thematic/	No change
USGS	http://ne.water.usgs.gov/	No change
USGS	http://nrmsc.usgs.gov/	No change
USGS	http://nsdi.usgs.gov/	No change
USGS	http://nsmp.wr.usgs.gov/	No change
USGS	http://nsmp.wr.usgs.gov/GEOS/geos.html	No change
USGS	http://ok.water.usgs.gov/	No change

Bureau	Web Page Address	Status as of April 17, 2001
USGS	http://online.wr.usgs.gov/kiosk/comments.html	No change
USGS	http://pa.water.usgs.gov/	No change
USGS	http://pdsimage.wr.usgs.gov/ATLAS.html	No change
USGS	http://pubs.usgs.gov	No change
USGS	http://quake.wr.usgs.gov/	No change
USGS	http://quake.wr.usgs.gov/research/internship.html	No change
USGS	http://ratbert.wr.usgs.gov/products/personnel.asp	No change
USGS	http://ratbert.wr.usgs.gov/products/personnel.aspy	No change
USGS	http://ris.wr.usgs.gov/	No change
USGS	http://rockyweb.cr.usgs.gov/	No change
USGS	http://s601dcascr.wr.usgs.gov/Sites/	No change
USGS	http://sc.water.usgs.gov/	No change
USGS	http://sd.water.usgs.gov/	No change
USGS	http://seeps.wr.usgs.gov/	No change
USGS	http://sfbay.wr.usgs.gov/	No change
USGS	http://sfbay.wr.usgs.gov/access/bioavail/	No change
USGS	http://sfbay.wr.usgs.gov/access/wqdata/	No change
USGS	http://sfgeo.wr.usgs.gov/	No change
USGS	http://srfs.wr.usgs.gov/	No change
USGS	http://srfs.wr.usgs.gov/library.htm	No change
USGS	http://srfs.wr.usgs.gov/projects.htm	No change
USGS	http://srfs.wr.usgs.gov/staff.htm	No change
USGS	http://time.er.usgs.gov/	No change
USGS	http://tn.water.usgs.gov/	No change
USGS	http://toxics.usgs.gov/	No change
USGS	http://tundra.wr.usgs.gov/wrmrsAK	No change
USGS	http://tx.usgs.gov/	No change
USGS	http://usgsprobe.cr.usgs.gov/	No change
USGS	http://ut.water.usgs.gov/faq/faq.html	No change
USGS	http://ut.water.usgs.gov/infores/gwdatareq.html	No change
USGS	http://ut.water.usgs.gov/infores/sfdatareq.html	No change
USGS	http://ut.water.usgs.gov/infores/wqdatareq.html	No change
USGS	http://ut.water.usgs.gov/infores/wwwquestion.html	No change
USGS	http://ut.water.usgs.gov/WR.UT.html	No change

Bureau	Web Page Address	Status as of April 17, 2001
USGS	http://va.water.usgs.gov/index.html	No change
USGS	http://volcanoes.usgs.gov	No change
USGS	http://vulcan.wr.usgs.gov/	No change
USGS	http://wa.water.usgs.gov/	No change
USGS	http://water.usgs.gov	No change
USGS	http://water.usgs.gov/nrp/proj.bib/	No change
USGS	http://water.usgs.gov/software/	No change
USGS	http://webdata.fsl.orst.edu/fresc/administrative/current.php	No change
USGS	http://wildfire.usgs.gov/	No change
USGS	http://woodshole.er.usgs.gov/operations/sfmapping	No change
USGS	http://wrgis.wr.usgs.gov/docs/geologic/ Fort.Irwin.ES.web/Fort.Irwin.html	No change
USGS	http://wrgis.wr.usgs.gov/docs/gump/gump.html	No change
USGS	http://wrgis.wr.usgs.gov/docs/parks/project/interp.html	No change
USGS	http://wrgis.wr.usgs.gov/king-sized-coprolite.html	No change
USGS	http://wrgis.wr.usgs.gov/MojaveEco/	No change
USGS	http://wrgis.wr.usgs.gov/parks	No change
USGS	http://wrgis.wr.usgs.gov/techniques	No change
USGS	http://wrgis.wr.usgs.gov/wgmt/elnino/	No change
USGS	http://www.aqd.nps.gov/grd/usgsnps/project/home.html	No change
USGS	http://www.arcpartners.org/	No change
USGS	http://www.avo.alaska.edu/	No change
USGS	http://www.cac.gov/	No change
USGS	http://www.cerc.usgs.gov/	No change
USGS	http://www.cfr.washington.edu/research.usgs/cascadia/contact.htm	No change
USGS	http://www.cfr.washington.edu/research.usgs/cascadia/metadata.htm	No change
USGS	http://www.cfr.washington.edu/research.usgs/ cascadia/people/darryll.htm	No change
USGS	http://www.cfr.washington.edu/research.usgs/	No change
USGS	http://www.cfr.washington.edu/usgs/cascadia/	No change
USGS	http://www.fcsc.usgs.gov/	No change
USGS	http://www.geoall.net/	No change
USGS	http://www.geophys.washington.edu/USGS	No change

Bureau	Web Page Address	Status as of April 17, 2001
USGS	http://www.glsc.usgs.gov/	No change
USGS	http://www.gsdi.org/	No change
USGS	http://www.mbr-pwrc.usgs.gov/	No change
USGS	http://www.mesc.usgs.gov/butterfly	No change
USGS	http://www.mp1-pwrc.usgs.gov/	No change
USGS	http://www.mp2-pwrc.usgs.gov/	No change
USGS	http://www.pwrc.usgs.gov/	No change
USGS	http://www.usgs.nau.edu/carnivore/pres_org.htm	No change
USGS	http://www.usgs.nau.edu/staff/	No change
USGS	http://www.werc.usgs.gov/	No change
USGS	http://www.werc.usgs.gov/boxsprings/	No change
USGS	http://www.werc.usgs.gov/chis/index.html	No change
USGS	http://www.werc.usgs.gov/dixon/people.html	No change
USGS	http://www.werc.usgs.gov/gg/ggpeople.html	No change
USGS	http://www.werc.usgs.gov/hq/people.html	No change
USGS	http://www.werc.usgs.gov/lasvegas/people.html	No change
USGS	http://www.werc.usgs.gov/pb/people.html	No change
USGS	http://www.werc.usgs.gov/pt.reyes/index.html	No change
USGS	http://www.werc.usgs.gov/redwood/personnel.htm	No change
USGS	http://www.werc.usgs.gov/sandiego/people.html	No change
USGS	http://www.werc.usgs.gov/santacruz/people.html	No change
USGS	http://www.werc.usgs.gov/sdfs/people.html	No change
USGS	http://wwwaux.cerc.cr.usgs.gov/spmd/	No change
USGS	http://wwwnwql.cr.usgs.gov/	No change
USGS	http://wwwrcamnl.wr.usgs.gov/	No change
USGS	http://wwwrcolka.cr.usgs.gov/	No change
USGS	http://wy.water.usgs.gov/	No change
USGS	http://edcw2ks15.cr.usgs.gov/	No change

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL

Internet Complaint Form Address

http://www.oig.doi.gov/hotline_form.html

Within the Continental United States

U.S. Department of the Interior Our 24-hour

Office of Inspector General Telephone HOTLINE 1849 C Street, N.W. 1-800-424-5081 or Mail Stop 5341 - MIB (202) 208-5300

Washington, D.C. 20240-0001

TDD for hearing impaired (202) 208-2420

Outside the Continental United States

Caribbean Region

U.S. Department of the Interior
Office of Inspector General
Eastern Division - Investigations
4040 Fairfax Drive
Suite 303
Arlington, Virginia 22203

Pacific Region

U.S. Department of the Interior Office of Inspector General Guam Field Pacific Office 415 Chalan San Antonio Baltej Pavilion, Suite 306 Agana, Guam 96911 (671) 647-6060

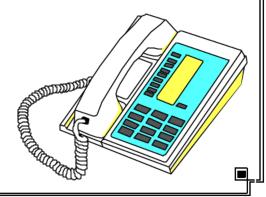
(703) 235-9221

HOTLINE

U.S. Department of the Interior Office of Inspector General 1849 C Street, NW Mail Stop 5341- MIB Washington, D.C. 20240-0001

Toll Free Number 1-800-424-5081

Commercial Numbers (202) 208-5300 TDD (202) 208-2420





U.S. DEPARTMENT OF THE INTERIOR OFFICE OF INSPECTOR GENERAL

EVALUATION REPORT

MOVING TO A CUSTOMER-CENTERED WEB PRESENCE





United States Department of the Interior

Office of Inspector General

134 Union Boulevard, Suite 510 Lakewood, Colorado 80228

7430

June 9, 2003

Memorandum

To: Chief Information Officer, Department of the Interior

From: Diann Sandy Wiann Sandy

Manager, National Information Systems Office

Subject: Evaluation Report on Moving to a Customer-Centered Web Presence

(Report No. 2003-I-0051)

The subject report presents the results of our evaluation of the Department of the Interior's (DOI) management and control of its Web sites. Although DOI has made some recent improvements, much remains to be accomplished. Specifically, the Department needs to manage its Web sites more efficiently, cost-effectively and securely; adhere to Federal laws and regulations; and focus on its customers.

We identified a framework for improvement based on practices employed by other Federal and state agencies as well as standards established by the Office of Management and Budget, the National Institute of Standards and Technology, and industry. We recommend that DOI implement a plan, using the framework described in this report, to improve management of its web sites. Please provide a written response to the report by July 15, 2003.

The legislation, as amended, creating the Office of Inspector General requires that we report to the Congress semiannually on all reports issued, actions taken to implement our recommendations, and recommendations that have not been implemented.

We appreciate the cooperation provided by all DOI staff during our evaluation. If you have any questions regarding this report, please call me at (303) 236-9243.

MOVING TO A CUSTOMER-CENTERED WEB PRESENCE

TABLE OF CONTENTS

NUMBER OF WEB SITES NOT CONTROLLED	
SECURITY NOT ADEQUATE	
WEB SITES NOT COMPLIANT WITH FEDERAL LAWS AND REGULAT	IONS8
WEB SITES NOT FOCUSED ON CUSTOMERS	g
BUILDING ON DOI'S EFFORTS	13
WEB PRESENCE ACTIVITIES	13
More Needs To Be Done	14
FRAMEWORK FOR IMPROVEMENT	15
STARTING THE MANAGEMENT AND CONTROL PROCESS	15
MOVING TO A CUSTOMER-CENTERED WEB PRESENCE	17
Enhancing Security	21
RECOMMENDATION	22
Appendices	
APPENDIX 1, EVALUATION SCOPE AND METHODOLOGY	23
APPENDIX 2, DIAGRAM OF THE DEPARTMENT OF THE INTERIOR'S	
Web Presence	25
APPENDIX 3, DEPARTMENT OF THE INTERIOR'S	
"OTHER" WEB SITES	
APPENDIX 4, SCORECARD OF THE DEPARTMENT OF THE INTERIOR	
Web Sites	2.8

MOVING TO A CUSTOMER-CENTERED WEB PRESENCE

CHALLENGES FACING THE DEPARTMENT OF THE INTERIOR

The Department of the Interior (DOI) needs to take charge of its Web presence (use of the Internet through World Wide Web technology and commonly referred to as the Web) to:

- Control the current unmanaged growth of Web sites;
- Reduce security risks;
- > Comply with Federal requirements such as those governing privacy; and
- Focus on its customers citizens, businesses, other government entities, and internal users.

NUMBER OF WEB SITES NOT CONTROLLED

DOI needs to reign in the proliferation of its Web sites to assure that Web site content and information are coordinated among bureaus and offices to minimize duplication, inconsistency, and redundancy of information. We found that DOI does not have a comprehensive inventory of its Web sites or of other components of its Web presence. (See Appendix 2 on page 25 for a diagram of DOI's Web presence). Using software (Web crawler) that automatically fetches Web sites, we estimated that DOI currently has approximately 31,000 Web sites presenting between 3 to 5 million pages of information. Figure 1 shows the percentage of Web sites maintained by major components of DOI. Appendix 3 on page 27 provides information on the sites classified as Other DOI Web Sites identified in Figure 1.

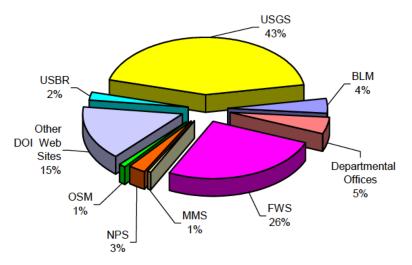


Figure 1. Distribution of DOI's Web Presence.

To provide a sense of DOI's Web sites and pages, we mapped, using a Web crawler, a portion of DOI's home page and site, as shown in Figure 2.

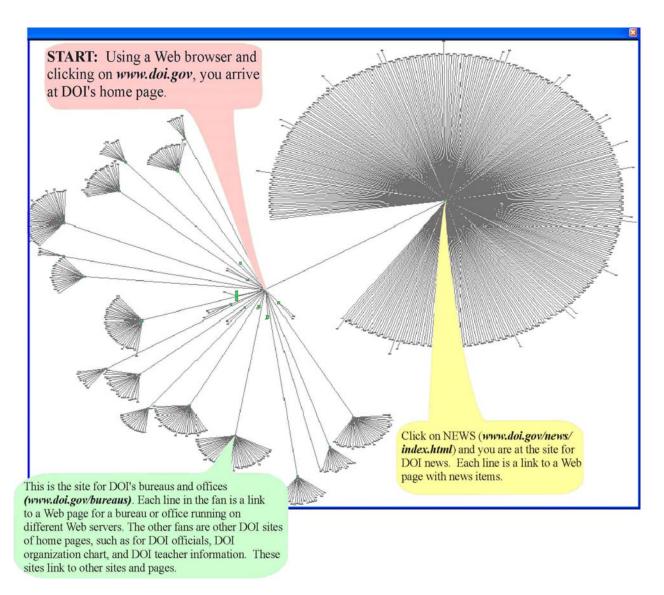


Figure 2. Snapshot of a Portion of DOI's Web Presence.

ANNUAL SPENDING ESTIMATED BETWEEN \$110 MILLION TO \$220 MILLION

We researched industry standards and practices and analyzed the cost of current DOI contracts for outsourcing and maintaining Web sites to develop our cost estimate for annually maintaining DOI's Web presence. Our research of industry indicated that the average cost to operate and maintain a Web site is generally between \$100,000 to \$200,000 annually. The \$100,000 cost is for basic sites that have no supporting database, limited storage requirements, few individuals posting to the Web, and one domain¹. The average cost increases to \$200,000 annually based on the complexity of the site and the numbers of individuals posting information. For extremely complicated sites, the costs could reach \$500,000. These figures include the costs of acquiring:

- Information technology resources, such as computer hardware and software, necessary to operate and secure Web sites and internal networks.
- Human resources needed to design, maintain, and control Web site content and information and to manage Webrelated hardware and software.

Costs for DOI contracts ranged from \$55,000 annually (for managing content, interfaces to other Web sites, and access to a third-party Web server) to \$200,000 (for content management for mapping and geographic information capabilities and databases). DOI's contracts did not always include costs for hardware and software to operate its Web sites.

We conservatively estimated, based on 1,100 domains, that DOI's annual cost to operate and maintain its Web presence is \$110 million. Using a less conservative basis of \$200,000 per domain, DOI's annual cost could be as high as \$220 million.

CONTENT NOT CONTROLLED

DOI has an excessive amount of duplicated, inconsistent, outdated, and redundant information on its Web sites. For example:

On the Office of Aircraft Services Web site, www.oas.gov, chapters of the Departmental Manual, Code of Federal Regulations, and Office of Management and Budget circulars, bulletins, and memoranda are duplicated rather

¹ A domain is a set of network addresses that is organized in levels. The top level identifies purpose commonality (for example, the organization that the domain covers such as ".gov"). The second level identifies a unique place within the top level domain and is equivalent to a unique address (such as "doi.gov") on the Internet. Lower levels on the domain may also be used (such as "smis.doi.gov).

- than the Office of Aircraft Services creating links to the sites that maintain these documents, such as DOI's Webbased electronic library (http://elips.doi.gov).
- On a Bureau of Land Management's Web site, inconsistent information is provided to customers on the procedures to apply for adopting a wild horse or burro. On one Web page, the customer is informed that the application form could be downloaded, printed and completed, and mailed to the appropriate Bureau office or that the customer could apply online for adopting a horse or burro using the Internet. On another Web page, the customer is informed that he or she would have to contact the applicable Bureau field office to request the application form.
- We found that DOI Web sites were out dated or did not indicate whether the site was actively maintained, therefore not assuring that the information presented is current and relevant. For example, 8 sites had not been updated for more than a year and 27 sites did not indicate the date the site was last updated.
- Redundant information on the same DOI activities is located on numerous DOI Web sites and pages. We performed key word searches on bureaus' and offices' Web sites of selected activities that were identified on DOI's home page. The analysis, as presented in Figure 3, showed that information on the same topic is presented on hundreds and thousands of Web sites by the seven major bureaus and offices.

	Number of Sites and Pages by Bureau With Information on the Same Activity						
DOI BUSINESS ACTIVITY	OSM	MMS	USGS	BOR	NPS	BLM	FWS
Endangered Species	125	103	1,154	294	1,000+	3,776	1,000+
Fisheries	0	0	2,892	287	892	2,096	1,000+
Habitat Conservation	0	0	288	13	42	421	1,000+
Wildlife	384	209	87,063	701	1,000+	14,942	1,000+
Plants	204	312	25,978	760	1,000+	4,554	1,000+
Ground Water Resources	15	3	48,271	32	49	0	0
Water Supply	149	10	4,755	1,260	683	417	748
Water Reclamation and Reuse	5	0	5	45	10	2	20
Oil and Gas	50	530	3,422	0	298	6,431	872
Petroleum	35	238	5,283	64	363	855	445
Helium	0	0	598	0	52	201	0
Hydroelectric	0	0	1,031	547	315	109	356
Renewable Energy	0	0	49	7	98	72	23
Energy Resources	37	44	2,012	5	74	206	45

Figure 3. Results of Queries on Bureaus' and Offices' Web Sites.

PROFESSED INFORMATION NOT ALWAYS AVAILABLE Web sites and links were not available as presented. For example:

- Web sites that were no longer accessible by the customer were not removed. For example, instead of being linked to the selected information, customers visiting www.doi.gov/searchall.html were informed that the Web site was no longer available and to notify a Web master of the problem. Although we brought these problems to the attention of Web masters, such as webteam@nbc.gov, links to these Web sites were not removed.
- Links to Web sites resulted in the customer receiving notice that the site could not be found. For example, on DOI Web site, www.doi.gov/business, we were not able to access five Web sites under the National Business Center.

We believe these problems can be attributed to the fact that DOI has inadequate and inconsistent configuration and content management controls. We noted that DOI has not assigned responsibility for managing Web content to ensure that information is properly and consistently presented and that information is not duplicated.

Further, we found that there was limited coordination between Web site managers to ensure that links to other Web sites and pages were available and for periodically testing linked Web sites for availability.

SECURITY NOT ADEQUATE

DOI does not have adequate security to safeguard its Web presence and its networks. We ascribed this condition to the lack of uniform Web security policies, procedures, and controls and the lack of standard configuration management. This increases DOI's security risks. For example, we found that:

- Individuals could identify network devices from the Internet by using readily available network surveying software tools. This increases the ability of individuals to compromise these devices and obtain unauthorized access to DOI's networks. For instance, using one of these tools, we identified the following devices in three of the Bureau of Land Management's networks:
 - o 2 Web servers
 - o 2 E-mail servers
 - o 6 firewalls
 - o 12 File Transport Protocol servers
- Web sites maintained by or for third parties did not have adequate security safeguards. DOI has no specific policy or control technique for outsourcing or hosting Web sites or restricting the registration of domains outside of the government domains (".gov" or ".fed.us"). When DOI sites are hosted on thirty party networks or when DOI hosts third parties' Web sites, there is little assurance that an interconnection between the third parties' networks and DOI's networks is not created. Security risks increase under these types of arrangements and should be mitigated through safeguards specified in contractual agreements. We identified:
 - Web sites that were hosted by commercial third parties and were not within the government domains. For example, a National Park Service Web site, www.windowsintowonderland.org, is hosted on a commercial third-party's server. In addition, the site was not under DOI's control because the site was not operating on a DOI IP (Internet Protocol) address.

- Web sites that were hosted by commercial third parties and were within the government domains did not have contractual agreements. As such, DOI lacks assurance that its Web sites were protected from access from the multiple other Web sites that were operating on the third-party's server. For example, Bureau of Land Management's "Adopt a Horse" Web site, www.adoptahorse.blm.gov, was managed by a contractor and was hosted on a third-party's server but a contract did not exist for the hosting services.
- o DOI was hosting Web sites for not-for-profit organizations, which may not be bound by the same security requirements as the Federal Government. For example, the Bureau of Reclamation hosted the Platte River Endangered Species Partnership (www.platteriver.org) and the Geological Survey's Northern Prairie Wildlife Research Center hosted six not-for-profit sites including the North American Reporting Center for Amphibian Malformations (www.npwrc.usgs.gov/narcam). This increases the risk to DOI's networks because third parties have access to update their Web sites.
- DOI was posting sensitive information on its Web sites. For example, the Minerals Management Service had information related to vulnerabilities of Supervisory, Control and Data Acquisition systems for offshore oil and gas production.
- Numerous types of Web server software with various versions and updates were operating throughout DOI. This increases the risk to DOI networks because known vulnerabilities in older versions of the software may not have been mitigated. Also, it creates inefficiencies in configuration management because each Web server's software must be individually evaluated, tested, and updated. In addition, DOI's ability to consolidate servers for central management and control may be inhibited because of these differences. Using network-surveying tools we identified that DOI has approximately 500 Web servers. We also obtained information on 405 of these servers indicating that DOI has at least three major types of Web server software with multiple versions of each type, as shown in Figure 4.

Apache		Microsoft IIS	Netscape-Enterprise Server	
Current Ve	ersion: 2.0.45	Current Version: 5.0	Current Version: 6.1	
Version	ns Installed	Versions Installed	Versions Installed	
1.1.1	1.3.26	3	2*	
1.2.5	1.3.27	4	3.6**	
1.2.6	1.3.9	5	4	
1.3.11	1.3a.1		4.1	
1.3.12	1.3b6		6.0	
1.3.17	2.0.39			
1.3.19	2.0.40			
1.3.20	2.0.42		* Netscape-Fastrack	
1.3.22	2.0.43		**Service Pack (SP) levels applied from no SP to SP3	
1.3.23	2.0.44			

Figure 4. Sample of Web Server Software Installed on DOI Web Servers.

DOI Web server configurations (file structures) could be mirrored using network-surveying software, such as a Web crawler. This is a problem because information on Web server configuration allows an individual to easily determine specific vulnerabilities and launch attacks against Web sites. In addition, it allows Web files that were not intended to be used by customers to be at risk of disclosure and misuse.

WEB SITES NOT COMPLIANT WITH FEDERAL LAWS AND REGULATIONS

DOI's Web sites do not always comply with Federal laws and regulations pertaining to the privacy of its customers and accessibility to information by persons with disabilities. For example, we found that:

- At least one Web site (pages www.blm.gov/nstc/soil/ Kids/adopt.html and www.blm.gov/nstc/soil/Kids/ gallery.html) was not in compliance with the Children's Online Privacy Protection Act [15 U.S.C. Chapter 91 § 6502]. Specifically, the site did not require children under the age of 13 to obtain parental consent before submitting requested personal information.
- Three Web sites that issued persistent cookies (small Web server files stored on customers' computers) had no documented approval for use of these cookies, and only one of these sites disclosed the use of persistent cookies.

Eight of the nine primary access points (DOI and bureaus home pages) do not meet all the requirements of Section 508 of the Rehabilitation Act Amendments of 1998 [29 U.S.C. § 794 (d)]. These requirements include providing access to electronic information to employees and other individuals with disabilities.

WEB SITES NOT FOCUSED ON CUSTOMERS

DOI's Web sites, with some exceptions, do not focus on its customers and do not allow them easy access to DOI information and opportunities. We evaluated 70 DOI Web sites to determine whether they applied best practices in 34 customer service areas covering user help features such as search and index, service navigation features including maps and events, and other user-friendly attributes such as the capability to E-mail the Webmaster. We concluded that overall DOI Web sites were adequate for 11 features, in need of improvement for 12 features, and inadequate for 11 features (see Appendix 4 on page 28 for details).

We also compared DOI's home page with the Department of Health and Human Service's (HHS) home page. This comparison, Figures 5 and 6, demonstrates the difference between a Web presence that is bureaucracy-centered (what the government does – DOI) and one that is customer-centered (what the government can do for the customer – HHS).

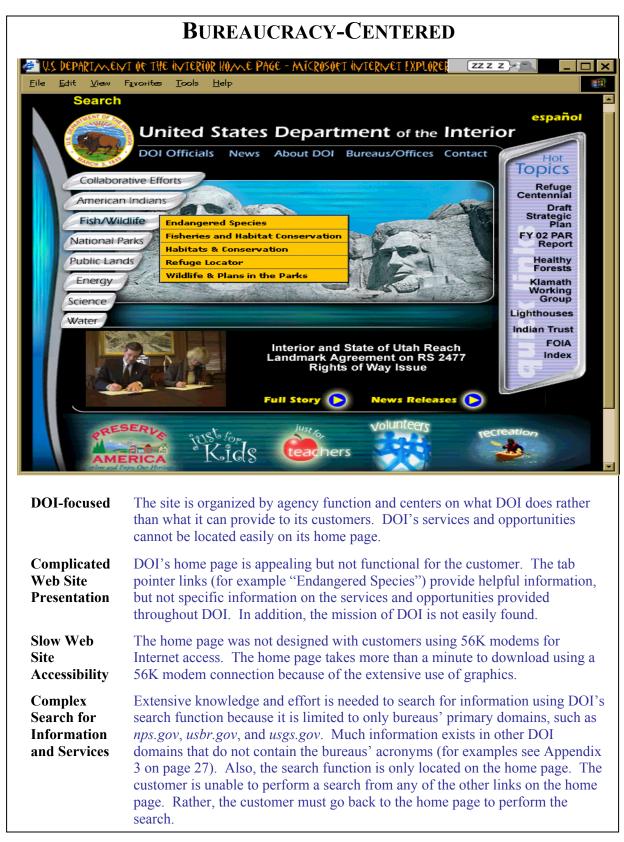


Figure 5. Department of the Interior's Home Page (Bureaucracy-Centered).

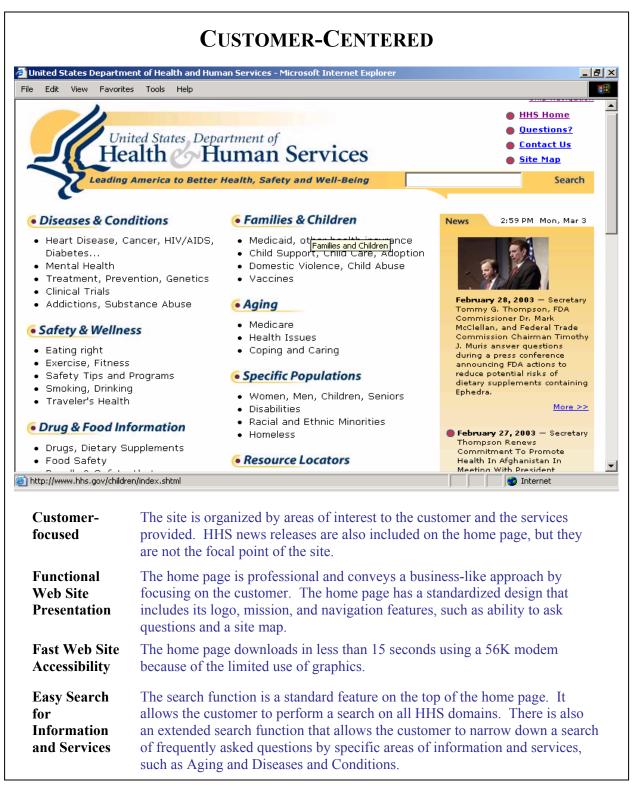


Figure 6. Department of Health and Human Services' Home Page (Customer-Centered).

BUILDING ON DOI'S EFFORTS

The goals of the President's *Expanding Electronic Government* (E-government) *Initiative* are to add value to customers' experiences with government and for government to better serve customers' needs while improving government efficiency. A key to accomplishing these goals is use of the Internet through World Wide Web technology. The purpose of a Web presence is to use Web-based resources cost effectively, deliver high-quality services, meet the needs of customers, comply with policies, and help accomplish missions and objectives. In the 1990s, the "World Wide Web" was released, and since then, the number of Web sites has grown exponentially, from an estimated 600 sites in 1993 to a million in 1997 and the number of sites continues to grow.

WEB PRESENCE ACTIVITIES

IMPROVEMENTS BEING MADE

Improvements by DOI include:

- Formalizing an E-government strategy team made up of senior level managers from the various program areas throughout DOI, Bureau and Office Chief Information Officers (CIOs), and field managers. The purpose of the team is to lead DOI's transformation to a customer-centered electronic service delivery provider, in accordance with customer and industry expectations, by using information technology (IT) to enable mission accomplishment, and to develop an E-government Strategic Plan.
- Addressing Web and electronic government requirements of the future in its Interior Enterprise Architecture.
- Beginning to consolidate Web servers and reducing the numbers of Internet access gateways.
- Implementing its policy requiring that all Web servers be contained in a Demilitarized Zone (DMZ).
- > Issuing policies to improve its IT security practices.
- ➤ Initiating projects to consolidate the access to information on some DOI Web sites to better provide opportunities to customers.

Considering the initiation of a project to implement a content management system.

SOME WEB SITES PROVIDE EASY ACCESS TO INFORMATION

We found that some of the DOI's Web sites have features which allow customers to easily locate specific information or to query for information through various techniques. For example, the U.S. Fish and Wildlife Service's home page allows the customer to select news articles by date and subject, the Bureau of Reclamation has a similar feature to aid customers in locating specific Reclamation manuals, and the Bureau of Land Management allows customers to submit requests and questions to the Bureau's Web team through a variety of electronic methods.

MORE NEEDS TO BE DONE

Despite these efforts, we believe that DOI needs to redesign its Web presence to focus on the customer, enhance security, maintain privacy, reduce duplication, and, at the same time, better manage its costs. To aid DOI in this endeavor, we developed and presented in the next section of this report a framework for improvement based on best practices identified through our reviews of various Federal and state agencies' Web sites; Federal agencies' Web procedures and practices; and Office of Management and Budget, National Institute of Standards and Technology, and industry standards.

FRAMEWORK FOR IMPROVEMENT

Our framework is based on a more centrally controlled and managed Web presence and focuses on ways for DOI to enhance its processes to not only improve its management of costs and security but also to aid in transforming its bureaucracy-centered Web presence to a customercentered Web presence.

STARTING THE MANAGEMENT AND CONTROL PROCESS

GETTING STARTED

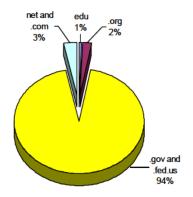


Figure 7. Distribution of DOI's Web Presence by Domain Type.

Six percent of DOI's Web domains are not government domains.

Inventory Web resources, justify domains and sites, and implement management controls over these resources. To accomplish these tasks, we suggest that DOI:

- Inventory IP addresses, Web domains and sites, and Web server operating systems and record the physical location of these resources. To help accomplish the inventory, DOI should issue a moratorium on new Web domains and sites except for urgent business reasons.
- Discontinue use of .org, .net, .com or other non-government domains where possible. If there is a need to use non-government domains, these should be supported by a business case and formally approved by the DOI CIO.
- Implement contracts for maintaining all outsourced and hosted Web sites and ensure that the contract language adequately addresses security requirements, including requirements to use DOI IP addresses, ensure that DOI's Web content is protected, and make sure that system configurations are consistent with DOI security policies and practices.
- Establish a position for and select a DOI Web Master. The position should report directly to the DOI CIO. The position's authority and responsibilities should include issuing and enforcing DOI policies and standards related to Web resources, such as approving all new Web domains, coordinating selection of content management software solutions and portal technologies, and Web server configuration.

- Require network management staff to coordinate with the DOI Web Master when assigning IP addresses for Web domains.
- Establish a position for and select a DOI Content Manager. We believe this position should be located within the Immediate Office of the Secretary to ensure DOI's Web sites appropriately present the Secretary's message. In addition, this position should issue and enforce policies to control the format and style of DOI Web sites, to establish an approval process for content published on Web sites, and to control the numbers of Web pages. This individual should have the authority to disable and remove pages from public access and manage information in accordance with DOI records policies. The Content Manager should also act as liaison between the DOI Web Master and all levels of program managers.
- Determine the need for all existing domains, Web sites, and Web pages and disable those that are not needed, not functional, or not accessible. Information on the Web should be based on the DOI enterprise lines of business. All DOI Web sites should be justified by business cases that include supporting metrics.
- Develop and implement DOI policies and standards to establish minimum controls for its Web presence. These policies and standards should ensure compliance with Federal laws and regulations. In addition, the policies should address Web page format, standardization, and content; training program for Web presence management; Web security; and operational procedures, such as change and configuration management. Policies should also include other areas such as cost/benefit analysis, E-mail inquiries, E-government initiatives, and hosting or outsourcing Web sites.

NEXT HURDLES

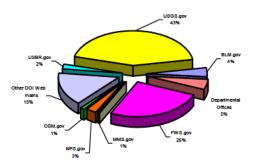


Figure 8. Distribution of the Known 1,100 DOI domains.

Fifteen percent of DOI's domains do not reside within DOI and Bureau/Office specific domains.

MOVING TO A CUSTOMER-CENTERED WEB PRESENCE

FOCUSING ON THE CUSTOMER

- ➤ Use the Web presence to focus on the customer by providing enhanced quality and availability of products, services, and opportunities; improved timeliness of information; better accessibility; and improved mission achievement. We suggest that DOI:
 - Identify the products, services, and opportunities that it offers customers, and identify those that could be made available through the Web.
 - Identify DOI customers and determine their wants and expectations.
 - Align or focus products, services, and opportunities toward customers. For example, on DOI's "Collaborative Efforts - Conserving Endangered Species through Partnerships" it informs customers of what the results were of partnership activities instead of how the customer could become a partner in this conservation program.
- ➤ Centrally locate access points to the existing products, services, and opportunities that customers want based on the results of the above suggestions. DOI should consider portal technology so that a customer who is not familiar with DOI can easily find specific information without extensive knowledge of DOI or the Web. (See Figure 3 on page 5 for business activities of DOI that can be found throughout DOI's Web presence at multiple access points.)
- ➤ Review current Web sites and pages for the characteristics listed below. Based on the results of the review, take action either by correcting the site or page or removing it. The review should determine whether:
 - o Information is timely.

- Information is accurate, consistent, and not redundant.
- Web pages are accessible within a reasonable amount of time via any connectivity method.
- Sites are accessible to all customers, to the maximum extent possible, by meeting Section 508 of the Rehabilitation Act Amendments of 1998.
- Privacy policies, including children's privacy, are easily reached on any Web access point.
- Information is not requested and collected from children without parental consent.
- Customers are notified upon departure from DOI sites.
- Persistent cookies are not used without the required approvals. The DOI CIO should disable Web sites that contain persistent cookies until the DOI Web Master is provided assurance that: (1) sites give clear and conspicuous notice of the use of persistent cookies; (2) there is a compelling need to gather the data on the site; (3) appropriate and publicly disclosed privacy safeguards exist for handling any information derived from the cookies; and (4) appropriate bureau or office heads or the Director of DOI's National Business Center have formally approved the use of each persistent cookie.

See Appendix 4 on page 28 for the results of our review of some of these features on selected DOI Web sites.

ESTABLISHING A STRATEGY

Develop an E-government strategic plan to use IT to transform the way DOI works to improve services to its customers. DOI should complete a strategic plan that includes:

- ➤ E-government mission and vision that aligns with DOI's Strategic Plan, IT Strategic Plan, and the Interior Enterprise Architecture objectives.
- Applicable legal requirements including security, privacy, and records management.
- Goals and associated objectives supporting the mission and vision.

- Metrics to measure performance for achieving the goals. These metrics should, at a minimum, measure:
 - Use of resources to maintain Web presence.
 - How well the Web sites meet the needs of customers.
 - How much the Web sites are contributing to customers taking advantage of the opportunities offered through DOI's Web presence and enabling DOI to better accomplish its mission.
- Short- and long-term steps and success factors to achieve the desired outcomes.

A best practice contributing to transforming from a bureaucracy-centered to a customer-centered Web presence is developing and implementing a strategy for managing Web content and design to focus on customers' wants. To achieve this transformation, we suggest that DOI develop Web content management and design policies and procedures that include:

- ➤ Periodically reassessing what customers want using methodologies such as analyzing: (1) systems logs, for example, to determine the numbers of times and the amounts of time each site is visited or is accessed; (2) key word searches; (3) frequently requested information; and (4) online customer satisfaction surveys.
- Creating a uniform look across DOI to include a standardized Web site design. The design should ensure that when Web sites are accessed the customer is made aware that it is a DOI Web site. While bureau-specific information can be provided, it should not confuse the customer that they are somewhere other than DOI. This can be accomplished by developing templates to standardize the look and feel of DOI Web sites and pages as well as filtering out unwanted content.

Ensuring Transformation Continues



Figure 9. Cycle To Ensure Web Presence Remains Customer Focused.

- Periodically evaluating the accessibility of the Web sites for broken links, orphan pages, connectivity issues, and user friendliness features, and ensuring deficiencies are corrected.
- Ensuring information that is posted on DOI Web sites is consistent, up-to-date, and not redundant.
- Moving or eliminating unnecessary or unwanted information not of interest to the public customer. Pertinent information for DOI employee users should be placed on a DOI intranet.
- ➤ Improving the efficiency of maintaining and posting information and the ability for users to customize the information they want by requiring, to the extent possible, pages to be dynamic (where information is found through queries to a database) rather than static (which is similar to hard-copy information where changes require rewriting the Web page).
- Defining what is sensitive information that should not be posted on the public Web sites.
- ➤ Standardizing all Web sites that are designed for children to include requirements for parental consent before information is requested and collected from children under the age of 13 thus complying with the Children's Online Privacy Protection Act.
- ➤ Ensuring privacy statements and Freedom of Information Act [5 U.S.C. § 552 as amended by Public Law 104-231, 110 Stat. 3048] procedures are accessible from each Web page and ensuring that disclaimer statements are consistent with the DOI Information Quality Guidelines.
- ➤ Ensuring information is grouped around lines of business and services and allowing access through portal technology rather than through multiple sites.

ENHANCING SECURITY

NEAR-TERM

Implement procedures to protect information and servers from loss, misuse, or modification and unauthorized access through minimizing vulnerabilities and mitigating threats to an acceptable level. To enhance the security of its Web sites, DOI should:

- Inventory Internet access points and eliminate or consolidate to reduce the total numbers of Internet access points throughout DOI.
- Document the Internet access points on network topologies, including connections to hosted and outsourced servers.
- Ensure that the required security architecture, which should include DOI Web sites and those sites that are outsourced and hosted, are in a DMZ.
- ➤ Develop a naming standard for hosts or network devices to prevent the easy identification of operating systems or functions from the Internet. For example, a device with the name "doi-firewall-sw" could easily be identified as a firewall.
- Perform periodic risk assessments on Internet access points and implement appropriate controls to protect internal networks.
- Perform risk assessments and privacy impact assessments prior to deployment of new Web sites.
- Ensure Web server software and related operating systems are updated with the most recent patches or fixes. (See Figure 4 on page 8 for current versions available of Web server software and examples of what is used on DOI Web servers.)

KEEPING DOI'S WEB PRESENCE SECURE

Establish configuration standards for DOI Web architecture and develop configuration management policies and procedures.

- Consolidate, physically and logically, DOI and bureau Web servers to the maximum extent possible.
- Ensure DOI's Web presence is addressed in security plans and is incorporated into the Certification and Accreditation process for DOI's networks.

Using our framework, DOI should be able improve its Web presence by focusing on the customer, enhancing security, maintaining privacy, reducing duplication, and, in the long term lowering costs.

RECOMMENDATION

We recommend that the DOI CIO develop and implement a plan, based on the framework identified in this report, for centrally controlling and managing DOI's Web presence.

EVALUATION SCOPE AND METHODOLOGY

SCOPE OF EVALUATION

Our evaluation included all the Department of the Interior's (DOI) and its components' (bureaus and offices) Web sites and pages that were available for access by the public and were connected to the Internet during November 2002 through March 2003. Web sites that were not available and therefore not included in our evaluation were those of the Bureau of Indian Affairs, the Office of Hearing and Appeals, and the Office of Special Trustee for American Indians. In addition, we limited our review of the Office of Indian Education .edu Web sites to determining the numbers of domains and Web sites. Office of Indian Education .edu Web sites were not subjected to Web presence analysis because they serve a different function than the other DOI sites. Finally, we limited our review to only http:// and https:// which are the basic means for customers to interact with the World Wide Web and to download requested information.

We reviewed DOI and its components' policies and procedures related to managing and controlling Web sites. We also interviewed DOI personnel responsible for maintaining Web sites and servers. We evaluated DOI processes and its publicly available Web sites and compared these to best practices that we developed from our reviews of various Federal and state agencies Web sites; Federal agencies' Web procedures and practices; and Office of Management and Budget, National Institute of Standards and Technology, and industry standards.

We performed this evaluation in accordance with the "Government Auditing Standards" issued by the Comptroller General of the United States. Accordingly, we included tests and other procedures that were considered necessary under the circumstances.

WEB DOMAINS AND SERVER REVIEW

To identify DOI's domains and Web servers and to determine whether security was adequate, we used several network surveying software tools to identify and analyze DOI's and its components' domains, Web sites, servers, and networks.

We used Web crawler software programs to identify DOI's Web domains and sites and Web site configurations. We also used these tools to identify Web sites hosted by DOI that may be unauthorized and DOI Web sites that were hosted outside of DOI. From this information, we identified DOI's IP addresses related to DOI's Web presence. In addition, we used a network-mapping tool to identify hosts that were not identified by the Web crawler tool. This tool also provided us with lists of hosts, servers, and other network devices such as routers, switches, firewalls, and printers that were identifiable from the Internet.

WEB SITE REVIEW METHODOLOGY

We developed a checklist based on identified best practices for Web site content and features (see Appendix 4 on page 28 for results of our evaluation). We evaluated these features on the following selected 70 Web sites:

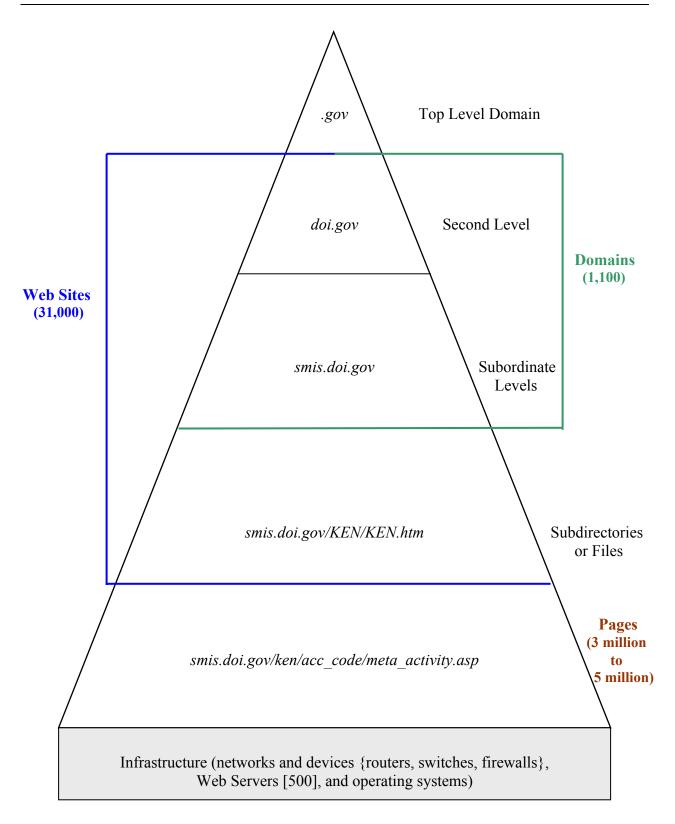
- 56 tab pointer links from the eight tabs listed on www.doi.gov Collaborative Efforts, American Indians, Fish/Wildlife, National Parks, Public Lands, Energy, Science, and Water
- > 9 bureau and DOI home pages
- > 5 judgmentally selected DOI and bureau Web sites

WEB SITES REVIEWED

Bureau	Number of Sites Reviewed
U.S. Geological Survey (USGS)	23
National Park Service (NPS)	9
Bureau of Land Management (BLM)	8
Minerals Management Service (MMS)	8
U.S. Fish and Wildlife Service (FWS)	7
Department of the Interior (DOI)	7
Bureau of Reclamation (BOR or USBR)	5
BLM and Forest Service	1
National Business Center (NBC)	1
Office of Surface Mining Reclamation and Enforcement (OSM)	1
Total	70

In addition to the 70 sites, we judgmentally selected numerous other DOI Web sites and pages. We reviewed these Web sites and pages for features, such as redundant, duplicated, sensitive, and inconsistent information; ease in accessing information; compliance with Federal laws and regulations; hosting other organizations' Web sites; and Web content and site design. Further, we evaluated business cases for selected DOI Web sites, if business cases were developed, and contracts and costs for DOI Web sites hosted on third-party Web servers.

DIAGRAM OF THE DEPARTMENT OF THE INTERIOR'S WEB PRESENCE



safety.oas.gov

DEPARTMENT OF THE INTERIOR'S "OTHER" WEB SITES

The Department of the Interior's (DOI) Web presence includes approximately 1,100 domains (addresses). Of these addresses, 15 percent do not include the "DOI" or bureau, such as "BLM," "NPS," or "USBR," acronyms as shown in Figure 1 on page 1 of the report. Examples of the "Other" Web sites follow:

americasoutdoors.gov handsontheland.gov partnersinflight.org anstaskforce.gov historicpreservation.gov pbin.nbii.gov baca.gov icbemp.gov permits.gov bacaranch.gov industrialecology.gov piedrasblancas.gov bianifc.org infms.gov pnwin.nbii.gov bioeco.gov interior.gov recreation.gov birdcon.nbii.gov invasivespecies.gov redondopeak.gov

cain.nbii.gov invasivespecies.nbii.gov reo.gov cal-parks.ca.gov lacoast.gov safenet.nifc.gov

cal-parks.ca.gov lacoast.gov cesu.org landfire.gov

cleanwater.gov lewisandclark200.gov sain.nbii.gov clear.search.gov liss.org science.gov clearinghouse1.fgdc.gov mbr.nbs.gov sciencerules.gov mesc.nbs.gov clearinghouse2.fqdc.gov seagrantnews.org clearinghouse3.fgdc.gov metadata.nbii.gov search.nbii.gov clearinghouse4.fgdc.gov mrlc.gov senrla.gov

cswgcin.nbii.gov msc.nbs.gov sierranevadawild.gov ec21.gov nationalatlas.gov sierrawildbear.gov ein.nbii.gov nbii.gov snow.water.ca.gov emtc.nbs.gov nbs.gov urban.nbii.gov urban.nbii.gov

far.nbii.gov nemi.gov usfilm.gov fgdc.gov nepa.gov usitc.gov firejobs.gov nfpors.gov usparkpolicenyfo.gov

fireleadership.gov nifc.gov vallegrande.gov vallesgrandenationalpreserve.gov

gai.fgdc.gov nigc.gov vcnp.gov vcnp.gov gapanalysis.gov nrin.nbii.gov volunteer.gov gcmrc.gov nrtc.gov westnilevirus.nbii.gov

genetics.nbii.gov nwcg.gov wildlandfire.gov geocommunicator.gov nwfireplan.gov wildlandfires.gov wildlandfires.gov geomac.gov oas.gov wildlifedisease.nbii.gov geo-one-stop.gov oregontrail.gov windowsintowonderland.org

govworks.gov osti.gov yourland.gov

SCORECARD OF THE DEPARTMENT OF THE INTERIOR'S WEB SITES

We developed a rating system to evaluate specific features on Department of the Interior's (DOI) Web sites. Our ratings were determined from information collected from 70 DOI Web sites based on Office of Inspector General (OIG)-developed checklists containing specific best practices attributes. If the Web site had a specific attribute, it received a score of 5 and if it did not have the attribute it received a 0. Answers, such as "possibly," "somewhat," or "limited," received a score of 2.5. In addition to determining a rating score for each attribute, we developed a color-coded system to better depict the areas that were adequate, in need of improvement, or inadequate. The following table provides the color code, the corresponding rating interval, and description.

		Rating Score	Description
		0-2.0	Inadequate
COLOR KEY		2.01-3.75	In Need of Improvement
		3.76-5	Adequate
			Not Applicable

The following table is a summary of the results of our evaluation of DOI's Web sites by an OIG-determined sample group: DOI Tab Pointer Links found on DOI's home page, DOI and bureau home pages, and other judgmentally selected sites. The features we evaluated were categorized by User Help Features, Service Navigation Features, and Other User Friendly Attributes.

	DOI Tab Pointer Links	Home Pages	Other Sites	Overall Score
User Help Features				
1. Comments and Feedback				
2. Search				
3. Index				
4. Site Map				
5. About the Site				
6. Frequently Asked Questions (FAQ)				
7. Help				
Overall Ranking for User Help Features				
Service Navigation Features				
8. Welcome				
9. Just For Kids				
10. Maps				
11. In the Newsroom/In the News				
12. Freedom of Information Act (FOIA)				
13. Events				

	DOI Tab Pointer Links	Home Pages	Other Sites	Overall Score
14. What's New				
15. About Services				
16. Links to Other Agencies/Regions				
Overall Ranking for Service Navigation Features				
Other User Friendly Attributes				
17. Page does not link to intranet log-in				
18. Duplicate information not found on pages tested				
19. Information was current or not expired				
20. Contact information - Phone number and addresses available				
21. Obvious link to contact information				
22. No personally sensitive information on page				
23. Link to Privacy Policy statement				
24. External links with proper exit notices				
25. No persistent cookies				
26. Link to Disclaimer statement				
27. Site compliant Section 508 of the Rehabilitation Act				
28. Page links to next hierarchy (within Bureau)				
29. Home page has link to DOI				
30. Customers can E-mail the Webmaster				
31. Customers can E-mail the Pagemaster				
32. Customers can E-mail other individuals				
33. Foreign language access				
34. Easy to use and accessible				

GLOSSARY OF TERMS USED

\mathbf{A} - \mathbf{D}

COOKIE

A message given to a Web browser by a Web server. The browser stores the message in a text file on the users' computers. The message is then sent back to the server each time the browser requests a page from the server. The main purpose of cookies is to identify users and possibly prepare customized Web pages for them. Generally, there are two types of cookies, session and persistent. The session cookie exists only when the user is browsing the Internet. The persistent cookie exists during the time the user is browsing the Internet as well as after the user closes the browser.

DMZ

A Demilitarized Zone is a network configuration used to provide security while allowing Internet traffic to access services such as a Web site (http), file transport protocol (FTP) servers, electronic mail (E-mail), and Domain Name Servers (DNS). The DMZ is the first line of defense between the Internet and an organization's internal networks and is usually a combination of firewalls and other computer hardware or software devices.

DOMAIN

A domain is a set of network addresses that is organized in levels. The top level identifies purpose commonality (for example, the organization that the domain covers such as ".gov"). The second level identifies a unique place within the top level domain and is equivalent to a unique address (such as "doi.gov") on the Internet. Lower levels on the domain may also be used (such as "smis.doi.gov).

E-H

FIXES - SEE PATCHES

HOST

A computer that is attached to a computer communications network that can use services provided by the network to exchange data with other attached computers and networks.

HTTP

Hypertext Transfer Protocol is the standard Internet Protocol for the exchange of information using World Wide Web (Web) technology.

HTTPs

An extension of the *Hypertext Transfer Protocol* that is designed to transmit individual messages securely.

I-L

INTERNET

The Internet is a network of networks. It is a system of linked computer networks, international in scope, that facilitates data transfer and communication services, such as remote login, file transfer (FTP), electronic mail (E-mail), newsgroups, and the World Wide Web.

INTERNET ACCESS GATEWAYS OR POINTS

A network device interface that connects the internal network and the Internet to provide users connected to the internal private network access to the Internet. It allows traffic both ways and it is usually referred to as a gateway.

IP ADDRESS

Is the abbreviation for Internet Protocol address commonly referred to as an IP. It is a numeric address that is given to servers and hosts connected to the Internet. For servers, it is translated into a domain name by a Domain Name Server (DNS). For hosts, it is assigned by the Internet Service Provider (ISP).

<u>M-P</u>

NETWORK DEVICE

Any machine or component that attaches to a communications network. Examples of network devices include servers, firewalls, routers, switches, hubs, bridges, and modems.

ORPHAN PAGE

The name for a Web page that has been abandoned but still remains available.

РАТСН

A supplemental software code that, when installed to the original software program, fixes problems (bug). A patch can usually be downloaded off the Internet in order to fix a software problem or security vulnerability.

PORTAL TECHNOLOGY

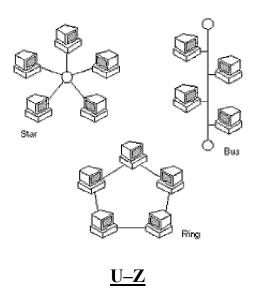
A technology strategy for facilitating the dissemination of information, providing self-service capabilities, and improving communications and interaction with and in between customers.

THREAT

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability. A threat can be either "intentional" (for example, an individual cracker or a criminal organization) or "accidental" (for example, the possibility of a computer malfunctioning or natural disaster such as an earthquake, a fire, or a tornado).

TOPOLOGY

The shape of a local-area network (LAN) or other communications system network. Topologies are either physical or logical. Three basic topologies are shown below:



URL

Abbreviation of *Uniform Resource Locator*, it is the global address of documents and other resources on the World Wide Web. The first part of the address indicates what protocol to use, for example *http*, and the second part specifies the IP address or the domain name where the resource is located.

For example, the two URLs below point to two different files at the domain *usbr.gov*. The first specifies an executable file that should be fetched using the File Transfer Protocol; the second specifies a Web page that should be fetched using the Hypertext Transfer Protocol:

ftp://ftp.usbr.gov/stuff.doc http://www.usbr.gov/main/index.html

VULNERABILITY

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system configured security policy.

WEB CRAWLER (ALSO KNOWN AS WEB SPIDER)

A program that automatically fetches Web pages. Crawlers or spiders are used to feed pages to search engines. Because most Web pages contain links to other pages, a crawler can start almost anywhere. As soon as the crawler sees a link to another page, it goes off and fetches that page. Large search engines, like Alta Vista, have many crawlers working in parallel.

WEB PAGE

A document on the World Wide Web. Every Web page is identified by a unique URL.

WEB PRESENCE

An organizations' established World Wide Web existence, through Web sites or a collection of Web files. It includes all components needed to provide the information published or posted on Web sites to be accessed or used by customers.

WEB SERVER

A Web server or Internet server is a computer that stores files of various types and makes them available over the Internet. A Web server stores the Web pages and provides them to users using Web "browser" software via the Internet.

WEB SITE

A location on the World Wide Web. Each Web site contains a home page, which is the first document users see when they enter the site. The site might also contain additional documents and files that may also be considered Web sites. A site can be owned and managed by an individual, company, or organization. This term is frequently used to identify anything located on the World Wide Web including a Web domain or a Web page within a domain.

WORLD WIDE WEB

A hypertext-based system for finding and accessing Internet-based data and information resources. It is capable of providing the public with user-friendly graphics-based access to information on the Internet. It is the most popular means for storing and linking Internet-based information.

How to Report Fraud, Waste, Abuse and Mismanagement

Fraud, waste, and abuse in government are the concern of everyone – Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or Insular Area programs and operations. You can report allegations to us by:

Mail: U.S. Department of the Interior

Office of Inspector General

Mail Stop 5341-MIB 1849 C Street, NW Washington, DC 20240

Phone: 24-Hour Toll Free 800-424-5081

 Washington Metro Area
 202-208-5300

 Hearing Impaired (TTY)
 202-208-2420

 Fax
 202-208-6081

Internet: www.oig.doi.gov/hotline_form.html





U.S. Department of the Interior Office of Inspector General 1849 C Street, NW Washington, DC 20240

> www.doi.gov www.oig.doi.gov



U.S. Department of the Interior Office of Inspector General

Evaluation Report

ANNUAL EVALUATION OF THE SECURITY PROGRAM AND PRACTICES OVER NON-NATIONAL SECURITY SYSTEMS, U.S. DEPARTMENT OF THE INTERIOR

REPORT NO. 2002-I-0049

SEPTEMBER 2002



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

September 16, 2002

Memorandum

To:

Secretary

From:

Earl E. Devaney

Inspector General

Subject:

Annual Evaluation of Information-Security-Program and Practices Over Non-

National Security Systems, U.S. Department of the Interior

(Report No. 2002-I-0049)

This report presents the results of our annual evaluation of the information security program and practices of the Department of the Interior (DOI) over non-national security information systems, as required by the Government Information Security Reform Act (GISRA).

We found that while DOI improved its security program during fiscal year 2002, much remains to be accomplished before it is in compliance with GISRA. Our report identifies shortcomings in security policies, procedures, and controls showing a material weakness in information security. Our report includes suggested improvements such as DOI's Chief Information Officer reporting directly to the Secretary.

Previously, our office provided to you and the DOI Chief Information Officer an executive summary of this report for inclusion in DOI's Annual Report on the Implementation of GISRA for fiscal year 2002.

If you have any questions about this report, please do not hesitate to call me at (202) 208-5745.

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

INTRODUCTION

This report presents the results of our evaluation of the Department of the Interior's (DOI) security program and practices over non-national security systems. The evaluation is required by the Government Information Security Reform Act (40 U.S.C. Chapter 25 § 1425) (GISRA). We concluded that the DOI is taking constructive actions to improve the security of its information technology (IT) systems, but that overall its security program does not adequately protect all information systems supporting DOI operations and assets. Until sound security policies and procedures are implemented, Bureau and office compliance with the security program is monitored, and security costs are fully integrated with the capital planning and investment control process, DOI should continue to report to the Congress the lack of an adequate information security program as a material weakness.

SCOPE AND METHODOLOGY OF EVALUATION

To complete our evaluation, we analyzed:

- Office of Inspector General (OIG) reviews performed during fiscal years 2001 and 2002 of security practices and general and application controls over 150 DOI IT systems¹ supporting telecommunications, energy and water operations including national critical infrastructure systems, scientific research and mapping, and financial operations; and a fiscal year 2002 review of DOI's IT capital planning process. (See Appendix 1 for systems covered by OIG reviews.)
- General Accounting Office and Office of Management and Budget reports issued during fiscal years 2001 and 2002 that addressed DOI IT security practices and controls.
- Examinations performed by contractors of the court-appointed Special Master² and by the major DOI components. The components consist of the Bureau of Indian Affairs (BIA), the Bureau of Land Management (BLM), the Bureau of Reclamation (BOR), the Departmental Offices (DO), the Minerals Management Service (MMS), the National Business Center (NBC), the National Park Service (NPS), the Office of the Special Trustee for American Indians/Indian Trust Management (OST), the Office of Surface Mining Reclamation and Enforcement (OSM), the U.S. Fish and Wildlife Service (FWS), and the U.S. Geological Survey (GS), hereinafter referred to as Bureaus.

¹ The OIG defined an IT system as an application or group of applications designed for specific sets of user requirements and general support systems that are under the same direct management control at locations included in our reviews.

² The U.S. District Judge presiding over <u>Cobell vs. Norton</u> appointed a Special Master to oversee the discovery process and administer document production, compliance with court orders and related matters.

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

➤ Internal reviews performed and documents provided by the major DOI components. (See Appendix 2 for a list of all reviews used in our evaluation.)

In addition to our analysis of other examinations, we reviewed the DOI's and the Bureaus' security management policies, procedures, and practices documents, such as security plans and security incident handling policies, and the most recent security plans for Bureau-defined mission critical systems. We also tested system security as part of our detailed review of general controls over IT security at GS. Additionally, we followed-up on our review of the national critical infrastructure systems completed in fiscal year 2001.

This evaluation was performed, as applicable, in accordance with the Comptroller General of the United States "Government Auditing Standards." Accordingly, we included such tests of records and other procedures that were considered necessary to accomplish our objective. In addition, we used the National Institute of Standards and Technology (NIST) Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," to evaluate the overall effectiveness of DOI's IT security program.

EVALUATION RESULTS

IT SECURITY
PROGRAM
IMPROVED BUT
MANY
SHORTCOMINGS
REMAIN

In fiscal year 2002, DOI took notable actions to improve its overall IT security program:

- In January 2002, the DOI Chief Information Officer (CIO) established an IT security team comprised of all of the DOI's IT security managers. The team developed plans and drafted and issued policy documents including a Critical Asset Valuation Guideline, Interim Response Reporting Process Guidance, security planning guides for general support systems and major applications, a contingency planning guide, and an IT system risk assessment guide.
- In April 2002, the DOI updated the Departmental Manual and revised its IT Security Plan to address overall DOI security policies and to establish implementation plans to improve the IT security program.
- In July 2002, the DOI CIO issued a mandate establishing specific requirements that must be implemented to secure DOI networks and data. The requirements included a strong password policy and control techniques that would strengthen the security of the DOI's networks and systems.
- In August 2002, the Secretary identified IT security as a top DOI priority and established and chartered the IT Management Council³ with a goal to:

... implement a model IT program capable of serving today's needs for sound investment management, in addition to providing the secure infrastructure needed to implement electronic government initiatives that will further enhance our ability to deliver better services and timely information to the American people.

³ The IT Management Council is Co-chaired by the DOI CIO and an elected Bureau CIO and the members are representatives from the BIA, BLM, BOR, FWS, GS, MMS, NBC, NPS, and OSM. In addition, the DOI's senior procurement executive will participate as a full voting member. The Council also includes ex-officio members from the DOI's Office of the Special Trustee, Office of Budget, Office of Financial Management, Office of Hearings and Appeals, Office of Inspector General, and Office of the Solicitor.

This report is exempt from disclosure to the public under the Freedom of Information Act, under Exemption 2 of the Act, 5 U.S.C. § 552(b)(2). For this reason, recipients of this report must not show or release its contents for purposes other than official review and comment under any circumstances.

By August 15, 2002, approximately 85 percent of all DOI employees and contractors completed IT security awareness training. In addition, the DOI CIO provided formal review training to prepare DOI employees with IT security responsibilities for the Certified Information System Security Professional examination and encouraged all IT security managers to become certified. Twenty-seven employees received the training and more than half received their certifications.

Despite these accomplishments, many shortcomings need to be addressed before IT systems and data are adequately protected. These issues are discussed in the sections that follow:

RESPONSIBILITIES
AND AUTHORITIES OF
PROGRAM OFFICIALS
FOR IT SECURITY
NEED TO BE
CLEARLY
COMMUNICATED

The responsibilities and authorities of GISRA and the Clinger-Cohen Act⁴ (44 U.S.C Chapter 35 § 3506) have not been clearly expressed to program officials. For example, in our review of annual performance plans for Assistant Secretaries and the CIO, we found that the plans for the Assistant Secretaries did not specifically require information security or information security management as a performance element. In our review of the Departmental Manual related to the responsibilities of program officials, such as assistant secretaries and Bureau heads, the responsibilities and authorities of the Clinger-Cohen Act and other Acts⁵ referred to in GISRA were not specifically identified. However, the Departmental Manual, "Information Technology Security Program," (considered the DOI's IT Security Program policy and revised in April 2002) did adequately describe the IT security management responsibilities under GISRA and the Clinger-Cohen Act for the Secretary, the DOI CIO and Office of the CIO, and the Bureau heads. That notwithstanding, our reviews of Bureau IT systems disclosed that program officials had not been held accountable for ensuring that the systems under their control met the minimum Federal security standards issued by the DOI, OMB, and NIST and consequently GISRA.

⁴ The Clinger-Cohen Act states "each agency program official shall be responsible and accountable for information resources assigned to and supporting the programs under such official." In addition, the Act requires that each agency shall implement and enforce applicable Governmentwide and agency information technology management policies, principles, standards, and guidelines.

⁵ Acts such as the Federal Financial Management Improvement Act which requires that agency financial management systems comply substantially with established system requirements and the Computer Security Act of 1987 which requires in part that "each Federal agency shall identify each Federal computer system and system under development, which is within or under the supervision of that agency."

DOI CIO NEEDS TO BE EMPOWERED TO **FULFILL ALL DUTIES** AND RESPONSIBILITIES OF A CIO

Although a DOI CIO has been formally designated by the Secretary and the position documented in the Departmental Manual, the CIO has not been empowered to fulfill all of the duties and responsibilities of the position, as required under GISRA and the Clinger-Cohen Act. The Clinger-Cohen Act requires the agency CIO (for agencies outside of the Department of Defense) to "report directly to such agency head to carry out the responsibilities of the agency." The Secretary delegated authority to the CIO to carry out the provisions of the Clinger-Cohen Act, but the Departmental Manual states that the CIO is only "responsible" rather than directly reports to the Secretary. Furthermore, the Departmental Manual, in describing the immediate office of the Secretary, does not include the CIO, thus further demonstrating that the CIO is not a member of senior management.

The Clinger-Cohen Act states that the designated CIO "shall head an office responsible for ensuring agency compliance with and prompt, efficient, and effective implementation of the information policies and information resources management responsibilities established." The CIO (Office of the Chief Information Officer) is in a staff position which reports to the Assistant Secretary for Policy, Management and Budget. Consequently, the CIO does not have the authority to enforce compliance by Bureaus with information security policies and ensure that Bureaus provided adequate resources to correct IT security weaknesses. In addition, the CIO is not a member of all IT-related senior-level decisionmaking councils, which inhibits the CIO's ability to effectively aid the Secretary in identifying DOI IT security needs and in initiating strategic IT security initiatives.

BUREAU CIOS AND NEED MORE AUTHORITY

Bureau CIOs and security managers lacked authority to effectively SECURITY MANAGERS carryout the program. One Bureau indicated that it did not have a position for a permanent CIO. Further, according to the Departmental Manual, only one Bureau CIO reports directly to the Bureau head and for two Bureaus, the Departmental Manual had not designated CIOs. We also found that most Bureau CIOs report to the Assistant Directors for Administration or are the Assistant Directors for Administration and Chief Financial Officers.

> Bureau IT security managers were not always properly placed in the organization or otherwise authorized to fulfill their responsibilities. For example, we found that five IT security managers did not report directly to the Bureau CIO. We also noted that, according to the Departmental Manual, one Bureau IT security manager was not authorized to perform reviews of IT systems outside the manager's immediate division. Furthermore, although the DOI IT Security Program policy requires that a full time Bureau IT security manager

be appointed, we found that seven IT security managers had collateral duties, such as individual IT system security management and IT system administration.

We also noted that program officials have not always ensured that personnel assigned individual IT system administration and IT system security responsibilities were qualified and trained to adequately fulfill their duties and responsibilities. For example, we found that a system owner was designated as the individual responsible for the security management of a system, rather than a specific system security administrator being designated. We also found that data owners were not provided sufficient training in performing security-related job functions.

DOI'S INFORMATION SECURITY PLAN NEEDS TO BE PRACTICED FOR EACH SYSTEM Despite a requirement to do so, not all the Bureaus have developed security plans for all their IT systems. The primary reason for this condition is that all systems have not been identified; and the sensitivity and criticality of these systems in relation to DOI operations and assets has not been determined. For example, one DOI contractor identified more than 500 systems, excluding general support systems such as wide area and local area networks in the DOI. Yet, DOI's fiscal year 2003 IT investments submitted to OMB for funding identified only about 150 systems.

To address the system inventory problem, the DOI CIO formed a team comprising the Office of the CIO and Bureau representatives to identify systems and determine the systems' criticality. Further action is needed to ensure that the DOI IT security plan is practiced throughout the lifecycle of each system, including holding program officials accountable for identifying the systems under their control, determining the sensitivity and criticality of each system in relation to the operations and assets supported by the systems, and developing IT security plans for each of the systems under their control. In addition, Bureau heads should be held accountable for developing Bureau-wide security plans to address this process. Further, the CIO should develop a process to verify that the DOI IT Security Program policy and IT Security Plan is implemented, updated, and practiced throughout the lifecycle of each system.

BUREAUS IT
INVESTMENTS NEED
REVIEW AND
CONCURRENCE BY
THE DOI CIO

The DOI's capital asset planning and investment control process was informal and Bureaus were able to make IT investments without review and concurrence of the DOI CIO. During fiscal year 2002, DOI began to implement a formal capital asset planning process and to better identify IT investment projects from a DOIwide perspective. The new process, however, did not provide for review and concurrence by the DOI CIO for all IT investments. Rather, the reviews were performed by multiple DOI executive councils which did not always include the DOI CIO. Further. Bureaus were allowed to make IT capital investments without concurrence of the DOI CIO for investments under specific dollar thresholds, such as investments in non-financial systems valued at under \$5 million. Our report (No. 2002-I-0038) on the DOI's IT capital asset planning process presents our suggestions on ways to improve DOI's process. We also determined that the DOI CIO has little control and oversight authority over Bureaus' IT security budgets and priorities. In a related matter, we found that the Bureaus had not identified the full lifecycle costs for IT investments including IT security costs. Therefore, the requested funding amounts in DOI's capital asset plans did not reflect the resources, such as infrastructure, people, and technologies, necessary to implement and institutionalize adequate security for each DOI system.

SECURITY PROGRAM NEEDS TO BE WELL INTEGRATED WITH CRITICAL INFRASTRUCTURE PROTECTION RESPONSIBILITIES The DOI IT security program is not well integrated with critical infrastructure protection responsibilities. The Office of Law Enforcement and Security is responsible for the DOI critical infrastructure program and has overall responsibility for personnel, physical, and operational security. The DOI CIO is responsible for overall IT security. BOR is responsible for integrating personnel, physical, operational, and IT security for three of the four DOI national critical infrastructures and the three national critical infrastructure systems. In a fiscal year 2001 audit (No. 2002-I-0004) and a fiscal year 2002 follow-up review of the security management over IT systems supporting energy and water operations, we concluded that BOR's integration of security responsibilities was not adequate and that corrective action to better integrate IT system security with physical and operational security in its protection and contingency planning documentation had not been completed.

DOI has not completed a project matrix review. Instead, it used an alternative method, based on Presidential Decision Directive 63, to identify national critical infrastructures and systems. DOI has issued its Critical Asset Valuation Guideline and is developing its enterprise architecture which should aid DOI in identifying any other IT systems that support critical operations and assets and in identifying the interdependencies and interrelationships between the IT systems and operations and assets. However, Bureaus have not implemented the Critical Asset Valuation Guideline and the DOI has not complete its enterprise architecture or ensured that all IT systems are identified. Therefore, DOI lacks assurance that the appropriate security technologies needed to protect its IT systems supporting critical operations and assets have been implemented.

GUIDANCE FOR
REPORTING
SECURITY INCIDENTS
AND SHARING
INFORMATION NEEDS
TO BE CLARIFIED
AND IMPLEMENTED

The DOI's revised IT Security Program policy and its "Interim Response Reporting Process Guidance" provide adequate general definitions of a security incident and determination of the severity of an incident. The policy and guidance, however, does not ensure that unsuccessful attempts to compromise a system or that low severity level incidents would be reported and tracked. Specifically, the guidance did not require that installation or regional IT security managers report low severity level incidents or unsuccessful attempts to Bureau IT security managers. Therefore, there is a risk that repeated low-level incidents or unsuccessful attempts, indicating a potential larger problem, may be occurring throughout a Bureau or DOI and not be investigated and reported appropriately.

The guidance also does not clearly delineate the responsibilities for escalating incidents to higher-level management officials and law enforcement authorities. For example, the responsibilities of both the Bureau IT security manager and the DOI IT security manager include sharing incident information with FedCIRC, OIG and law enforcement authorities, depending on the level of severity of the incident. Also, discretion in classifying an incident may improperly delay reporting. For instance, if the incident is considered high severity, the Bureau IT security manager has up to 8 hours to report the incident to the DOI IT security manager. If the incident is considered medium severity, the Bureau IT security manager informs the DOI IT security manager in a monthly summary report.

8

⁶Project matrix review is used to determine the criticality of operations and assets, their interdependencies and interrelationships, and, how those operations and assets are secured.

Finally, we noted that full implementation of the policy and guidance has not been accomplished because of the recent April 2002 issuance of the policy and guidance and because only four bureaus had developed incident response policies.

COMPUTER
"PATCHES" NEED TO
BE TESTED AND
INSTALLED TIMELY

We did not find any evidence that the DOI and Bureaus had a means to confirm that patches⁷ had been tested and installed in a timely manner. We found that at least one Bureau did not test the patches because a test environment had not been established and at least seven Bureaus had not installed patches timely. Without testing patches prior to installation, the Bureaus could inadvertently damage DOI networks. In addition, without timely installation of patches, the networks and applications were subject to vulnerabilities that could be prevented had the appropriate patches been installed.

RISKS NEED TO BE ASSESSED AND THE APPROPRIATE LEVEL OF SECURITY DETERMINED Program officials have not assessed risks and determined appropriate levels of security to protect all IT systems. Although we found that some systems have been assessed, the assessments generally were not adequate because interconnections to systems of other Federal agencies; state, tribal, and local governments; and the public, often via the Internet, were not included. Further, until the Bureaus identify all their IT systems, there is no assurance that all security risks will be identified and addressed.

Without an adequate assessment of risks, program officials cannot determine the appropriate level of security required and whether the security controls and techniques were appropriate. This is not to say that the programs officials have not implemented IT security controls to safeguard IT systems. Rather, the IT security controls may not be appropriate to ensure risks are cost-effectively mitigated or acted upon. Finally, program officials may not always have a clear understanding of the residual risks being accepted.

SECURITY PLANS
NEED TO BE
PROPERLY
DEVELOPED AND
UPDATED FOR ALL
IT SYSTEMS

Although more IT system security plans were developed during fiscal year 2002 than in fiscal year 2001, program officials did not ensure that all IT systems under their control had up-to-date IT security plans. In addition, when IT system security plans were developed, the plans were generally inadequate because they:

⁷ A patch is a fix to repair a deficiency in the functionality of an existing routine or program, generally in response to an unforeseen need or set of operating circumstances. Patching is a common means of adding a feature or a function to a program until the next version of the software is released. For example, when security weaknesses in a computer operating system such as Microsoft Windows 2000 are identified, Microsoft corrects this problem by issuing a patch to be installed.

- Were not based on the sensitivity or criticality of the data and the operations and assets the IT systems supported.
- Were not based on risk assessments. For example we identified nine IT system security plans which were developed without any type of assessment of risks. Therefore, management could not ensure that controls identified in the plans were adequate to mitigate risks.
- Did not identify all of the interconnected systems. For example, system security plans for major applications did not consider connection to the Internet, Bureau wide-area networks, and the computer system where the application resided.
- Were not always formally approved by an appropriate senior management official.
- Were not periodically updated to reflect the current operating environment.
- For example, in one of the security plans reviewed the controls identified to protect the system from external networks were not supported by the existence of software or hardware devices to provide such protection.
- > Did not clearly identify persons responsible for security.

We also noted that the Bureaus lacked a process to ensure that the IT system security plans were updated at least every 3 years or when significant changes were made to the systems environment. For example, we reviewed 10 IT systems security plans supporting scientific research and mapping, and found that the plans were, generally in draft, developed during fiscal year 2002, and often the first plans developed even though the systems had been in operation in excess of 5 years. Also, some Bureaus believed that assessment of risks was not needed if systems were under development.

To help address these issues, the Office of the CIO is developing a Departmental certification and accreditation process for its IT systems which is planned for implementation in fiscal year 2003. However, an inventory of IT systems must be completed before a certification and accreditation process can by fully implemented across the Department.

NEED TO BE TESTED AND EVALUATED

SECURITY CONTROLS DOI is still developing methods to better test and evaluate IT security controls and techniques. As a result, Bureaus principally evaluate IT security controls using the management control review process established under OMB Circular A-123, Management Control and Accountability. As identified in our fiscal year 2001 GISRA report, these management control review checklists did not provide the level of review needed to sufficiently determine whether the implemented security controls and techniques were operating effectively. The DOI CIO released a draft bulletin that supported using NIST Special Publication 800-26 guidelines, the OMB required methodology, for performing IT system control reviews. However, while many of the Bureaus are in the process of performing reviews, they indicated that not all of the reviews were based on the required OMB methodology.

> In addition, we found contingency plans were not adequate or tested for at least 27 of the 75 systems we reviewed in fiscal year 2002. The lack of adequate testing and evaluation of security controls and techniques is evidenced by DOI's loss of the Internet connection in December 2001, the continual identification of weaknesses in IT security controls through penetration testing of the DOI's systems by contractors of the Special Master, and significant weaknesses in the Bureau's implemented security controls and techniques noted in OIG reviews.

SECURITY CONTROLS FOR CONTRACTOR PROVIDED SERVICES OR SERVICES PROVIDED BY OTHER **AGENCIES NEED TO** BE MONITORED

The DOI IT Security Program and IT Security Plan require the inclusion of appropriate language concerning IT security in contracts and memorandums of agreement or understanding. We found, however, that contracts for IT operations, such as application service providers, IT security and system administration, and software development and maintenance, did not have appropriate language. Consequently there was little assurance that adequate security controls existed and that the controls implemented met Federal requirements. We did note that at least three Bureaus that use service providers received reports related to the internal controls of the service providers' IT environment. These reports, while not specifically related to IT security, did address security issues such as controls over the operating systems, access procedures, and separation of duties.

ALL EMPLOYEES WITH SIGNIFICANT SECURITY RESPONSIBILITIES

The DOI CIO does not have a formal training program to ensure that all employees with significant IT security responsibilities receive appropriate training. By all employees with significant IT responsibilities, we mean Bureau IT security managers, system NEED TO BE TRAINED owners, installation or regional IT security managers, system administrators, system security managers, web masters, and system developers.

> The DOI CIO did establish a requirement and provide the capability for all system users to receive IT security awareness training during fiscal year 2002. Three Bureaus had their own computer-based training course and the remaining eight bureaus used the NBC's developed computer-based training course.

OTHER INFORMATION RELATED TO DOI'S IT SECURITY **PROGRAM**

The U.S. District Judge presiding over the Cobell vs. Norton case issued a temporary restraining order on December 6, 2001, prohibiting DOI to connect to the Internet because it could not demonstrate that Indian trust systems and data were adequately safeguarded. On December 17, 2001, the Court entered a consent order that provided the terms and conditions upon which DOI could seek the concurrence of the court-appointed Special Master to restore connections to the Internet. A key component of the process involved providing documentation to the Special Master that identified which IT systems housed or provided access to Indian trust data. Further, the consent order provided a means by which parts of DOI could reconnect to the Internet by providing assurance that IT systems connected to the Internet did not house or provide access to Indian trust data. As of August 31, 2001, not all DOI systems, such as those systems supporting operations of the BIA and the OST, have been approved to reconnect to the Internet. Further, the Special Master engaged contractors to conduct penetration tests of the DOI networks and systems. The contractors found that some systems which been reconnected to the Internet continued to have security weaknesses.

MATERIAL WEAKNESSES

The DOI reported the following material weaknesses for fiscal year 2001, including a significant number related to IT systems, as follows:

Material Weaknesses Reported

Description	Fiscal Year Reported
Inadequate Management of Trust Funds – OST*	1983
Inadequate Billing and Collection Over Irrigation Operations and Maintenance – BIA*	1984
Inadequate Debt Collection – BIA *	1987
Inadequate Acquisition Management Program – BIA	1989
Lack of Accountability and Control Over Artwork and Artifacts – DOI	1990
Inadequate Records Management – BIA and OST*	1991
Delivery of Federal Water to Ineligible Lands – BOR	1994
Deficiencies in Real Property Management - BIA	1995
Inadequate DOI-wide Maintenance Management Capability – DOI*	1998
Management and Oversight of the Land Exchange Program – BLM*	1998
Inadequate Internal Controls over Accounting Operations - MMS*	1999
Inadequate Management Controls and Audit Follow-up in the Federal Aid Program - FWS*	1999
Inadequate Wireless Telecommunications – DOI*	2000
Inadequate Structural Fire Program – NPS*	2000
Inadequate Land Inventory and Financial Reconciliations – BOR*	2000
Inadequate Computer Security – DOI*	2000
Administration and Oversight of the Wild Horse and Burro Program – BLM	1997; weakness considered corrected in fiscal year 2000 but reinstated as a material weakness in fiscal year 2001

^{*}Indicates material weaknesses directly or indirectly related to IT systems.

We reported in our fiscal years 2000 and 2001 Independent Auditor's Reports on DOI's financial statements that DOI had material weaknesses in internal controls related to financial reporting and had not complied with certain laws and regulations, as follows.

Description	Fiscal	Fiscal Year 2001
<u>Description</u> Internal Controls	<u>Year 2000</u>	<u>1 ear 2001</u>
Account Analysis and Reconciliation	X	x
•	X	^
Construction-in-Progress	X	х
Unliquidated Obligations	X	^
Lands and Land Rights Accruals	X	
		v
Trading Partners	X	X
Property, Plant, and Equipment	X	X
Financial Management and Accounting Processes at Minerals Management Service	X	
Security and General Controls over Financial Management Systems	X	х
Indian Trust Funds	X	х
Budgetary Data Reporting	X	
Compliance with Laws and Regulations		
Debt Collection Improvement Act of 1996	X	Х
Office of Management and Budget Circular A-11	X	
Prompt Payment Act	X	x
Federal Financial Management Improvement		
Act		
Accounting Standards		Х
Stewardship Investments	X	
Cost Accounting	X	
Financial Management System	v	х
Requirements	X	٨
United States Government Standard General		х
Ledger		^
Section 113 of Public Law 104-208 –		х
Advances for Interior Franchise Fund		

In addition, because DOI has not ensured that all IT systems have security plans and that an enterprise architecture was developed, DOI is not in compliance with:

- Computer Security Act of 1987
- Clinger-Cohen Act of 1996
- Government Information Security Reform Act.

COMMENTS ON THE DOI PLAN OF ACTION AND MILESTONES

Our review of the DOI's and the Bureaus' July 31, 2002 plans of action and milestones (POA&M) to correct IT security weaknesses noted the following deficiencies:

- Specific weaknesses identified by the OIG and external evaluators such as NIST's Computer Security Expert Assist Team (CSEAT) and the Special Master were not separately reported, but were grouped together as overall general weaknesses.
- Individual system weaknesses were reported as part of an overall bureau weakness, such as lack of security plans, risk assessments, and certification and accreditation; and specific systems were not included. Because weaknesses were rolled up, incremental steps to address system specific weaknesses were not included.
- Actions requiring multiple years to correct the weaknesses showed only a final completion data and the incremental milestone dates had not been established to effectively measure progress.
- Milestone dates or resources required to accomplish corrective actions were not always presented.

As a result, the plans of action and milestones could not be effectively used as a management mechanism to prioritize, track, and manage all efforts needed to close security performance gaps.

SUGGESTED Improvements

We suggest that DOI consider the following actions:

- **IMPROVEMENTS** 1. Include security management as a performance element in the annual performance plans of applicable program officials.
 - 2. Include in the Departmental Manual the specific responsibilities which are set forth under GISRA and the Clinger-Cohen Act for applicable program officials.
 - 3. Hold program officials' accountable for carrying out their information security responsibilities.
 - 4. Authorize the DOI CIO to report directly to the Secretary and include the CIO as a member of senior-level decision making councils concerning information technology.
 - 5. Remove the Office of the CIO from the offices of the Assistant Secretary for Policy, Management, and Budget.

- 6. Authorize the DOI CIO to be the approving and responsible official for all DOI IT-related councils and charters.
- 7. Hold subordinates of Bureau heads accountable for fulfilling their information security responsibilities.
- 8. Give Bureau CIOs sufficient authority to enforce security policy and relieve them of collateral duties.
- 9. Clarify guidance for reporting security incidents to ensure that all incidents or potential system compromises are reported.
- 10. Complete expeditiously the identification of Bureau IT systems and valuations.
- 11. Have Bureau IT security managers report directly to the Bureau CIO, provide security managers with sufficient authority to fulfill all their duties, and relieve them of collateral duties.
- 12. Establish a process to validate that all Bureaus have effectively implemented Federal and DOI policies and procedures, standards, and guidelines for all DOI systems.
- 13. Authorize the DOI CIO to oversight Bureaus IT security budgets and priorities.
- 14. Establish a review process to ensure that all IT capital asset plans for IT investments include IT security requirements and costs for the full life cycle of the IT investments.
- 15. Standardize policies and procedures for personnel, physical, operational, and IT security across DOI.
- 16. Establish a process to notify IT security personnel of patches available and controls to ensure that patches are tested and installed timely.
- 17. Establish a process to periodically evaluate contractor and other agency provided IT services to ensure IT security controls meet Federal standards.
- 18. Establish and periodically present a training program that addresses the training requirements needed for each position with significant IT security responsibilities, including program officials and systems owners.
- 19. Include in the POA&Ms all necessary steps and specific completion dates to address all known IT security weaknesses.

APPENDIX 1

SYSTEMS REVIEWED BY OIG AS PART OF ITS EVALUATION OF INFORMATION SECURITY PROGRAM AND PRACTICES OVER NON-NATIONAL SECURITY SYSTEMS, DEPARTMENT OF THE INTERIOR

	Systems Reviewed		
Bureau/Location	Fiscal Year 2001	Fiscal Year 2002	
Financial and Financial Related			
National Business Center (NBC), Denver, CO	Mainframe, Federal Personnel Payroll System (FPPS), Federal Financial System (FFS), Interior Department Electronic Data Acquisition System (IDEAS), and local area networks (LAN)	Mainframe, FPPS, FFS, IDEAS, and LANs	
NBC as accounting office for Departmental Offices, Denver, CO	FFS	FFS	
NBC, Reston, VA	Hyperion	Hyperion	
U.S. Geological Survey (USGS), Reston, VA	FFS, FPPS, IDEAS, LANs, and wide area network (WAN)	FFS, FFS, IDEAS, LANs, and WAN	
National Park Service, Herndon, VA	FFS, FPPS, IDEAS, LANs, and WAN	FFS, FPPS, IDEAS, LANs, and WAN	
U.S. Fish and Wildlife Service (FWS), Arlington, VA	FFS reporting to Hyperion	FFS reporting to Hyperion	
FWS, Denver, CO	FFS, FPPS, IDEAS, Real Property, LANs, and WAN	FFS, FPPS, IDEAS, Real Property, LANs, and WAN	
Bureau of Land Management, Denver, CO	FFS, FPPS, IDEAS, Collection and Billing System, LANs, and WAN	FFS, FPPS, IDEAS, Collection and Billing System, LANs, and WAN	
Bureau of Reclamation (BOR), Denver, CO	FFS, FPPS, IDEAS, Time Accounting System, LANs, and WAN	FFS, FPPS, IDEAS, Time Accounting System, LANs, and WAN	
Office of Surface Mining Reclamation and Enforcement, Denver, CO	Advanced Budget and Accounting Control Information System (ABACIS), FEEBACS, CPACS, IDEAS, FPPS, NT operating system, Unix operating system, LANs, and WAN	ABACIS, FEEBACS, CPACS, IDEAS, FPPS, NT operating system, Unix operating system, LANs, and WAN	

APPENDIX 1

	Systems Reviewed	
Bureau/Location	Fiscal Year 2001	Fiscal Year 2002
Minerals Management Service	ABACIS, LAN, WAN and	ABACIS, LAN, WAN and
(MMS), Herndon, VA	FFS	FFS
MMS, Denver, CO	Auditing Financial System	Minerals Revenue
	and LANs	Management System,
		Mainframe, LANs, and
		WAN
Bureau of Indian Affairs (BIA),	FFS, FPPS, IDEAS, LAN,	FFS, FPPS, IDEAS, LAN,
Reston, VA	WAN and Unisys	WAN and Unisys
BIA, Denver, CO	National Irrigation	NIIMS
	Information Management	
	System (NIIMS)	
BIA, Albuquerque, NM		Loan Management and
		Accounting System
BOR Energy and Water Includ		ructure
Technical Services Center,	LAN	
Denver, CO		
Boulder City, NV	Hoover Dam and Power	Hoover Dam and Power
	plant primary and	plant SCADA
	secondary Supervisory	
	Control and Data	
	Acquisition (SCADA)	
Sacramento, CA	Mid Pacific Region and	CVACS
	Central Valley Operations	
	Central Valley Acquisition	
	Control System (CVACS),	
	and LANs	
Folsom, CA	Folsom Dam CVACS	Folsom Dam CVACS
Shasta Lake City, CA	Shasta Dam CVACS	
Redding, CA	Keswick Dam CVACS,	
	Back-up CVACS, LAN,	
	and WAN and Spring	
	Creek Debris Dam CVACS	
Lewiston, CA	Trinity Dam CVACS,	
	Lewiston Dam CVACS,	
	and Whiskeytown	
	Dam/Judge Francis Carr	
	Power plant CVACS	
Grand Coulee, WA	Grand Coulle DAM	
	SCADA	
Boise, Idaho	Pacific Northwest Region	
	LANs, Hydromet, and	
	Agrimet	

APPENDIX 1

	Systems Reviewed	
Bureau/Location	Fiscal Year 2001	Fiscal Year 2002
Emmett, ID	Black Canyon Diversion	
***	Dam SCADA and LAN	
USGS Scientific Research an	nd Mapping	
Reston, VA		Reston LAN, Water
		Division Systems,
		Mapping Division
		Systems, Geologic
	{	Division Systems,
		Biological Research
		Division Systems, and
		GEONet3 WAN
Sioux Falls, SD		Distributed Ordering
		Research Reporting and
		Accounting Network, Earth
		Explorer, Windows NT
		operating system, and
		UNIX operating system
Denver, CO		National Water
		Information System
		(NWIS) Web and LAN,
		and Geologic Web and
		LAN
Golden, CO		U.S. National Seismic
		Network and LAN
Albuquerque, NM		NWIS, Global Seismic
		Network (GNS), GNS
		Web, and GNS LAN
Other		
FWS Region 6, Denver, CO	LANs and National	
	Communications Center	
Office of Inspector General,	LANs	
various locations		

APPENDIX 2

REVIEWS INCLUDED AS PART OF EVALUATION OF INFORMATION SECURITY PROGRAM AND PRACTICES Over Non-National Security Systems, DEPARTMENT OF THE INTERIOR

Office of Inspector General, Department of the Interior

- Advisory Report: Developing the Department of the Interior's Information Technology Capital Investment Process: A Framework for Action (August 2002).
- ➤ Independent Auditors' Report on the Departmental Office's Financial Statements for Fiscal Years 2001 and 2000 (April 2002).
- ➤ Independent Auditors' Report on the Interior Franchise Fund's Financial Statements for Fiscal Years 2001 and 2000 (April 2002).
- ➤ Independent Auditors' Report on the U.S. Fish and Wildlife's Financial Statements for Fiscal Years 2001 and 2000 (March 2002).
- Independent Auditors' Report on the Bureau of Reclamation's Financial Statements for Fiscal Years 2001 and 2000 (March 2002).
- ➤ Independent Auditors' Report on the Minerals Management Service's Financial Statements for Fiscal Years 2001 and 2000 (March 2002).
- ➤ Independent Auditors' Report on the National Park Service's Financial Statements for Fiscal Years 2001 and 2000 (March 2002).
- ➤ Independent Auditors' Report on the Bureau of Indian Affairs' Financial Statements for Fiscal Years 2001 and 2000 (March 2002).
- ➤ Independent Auditors' Report on the Office of Surface Mining Reclamation and Enforcement's Financial Statements for Fiscal Years 2001 and 2000 (March 2002).
- ➤ Independent Auditors' Report on the Bureau of Land Management's Financial Statements for Fiscal Years 2001 and 2000 (March 2002).
- ➤ Independent Auditors' Report on National Park Service Financial Statements for Fiscal year 2000, conducted by KPMG (January 2001).
- ➤ Advisory Letter: Department of the Interior Responses to Review Guide for Planning and Assessment Activities for Protecting Critical Non-Cyber Infrastructure (December 2001).
- Memorandum: September 30, 2000 Status of Recommendations Contained in Prior Office of Inspector General Audit Reports on General Controls Over Bureau of Indian Affairs Automated Information Systems (December 2001).
- ➤ Audit Report: Improvements Made in General Controls Over Automation Information Systems, Office of Surface Mining Reclamation and Enforcement (September 2001).
- Annual Evaluation of Information Security Program and Practices Over Non-National Security Systems, Department of the Interior (August 2001).
- Audit Report: Improvements Needed in Security Management of Information Technology Systems Supporting Energy and Water Operations, Bureau of Reclamation (November 2001).

APPENDIX 2

- Audit Report: Independent Auditors' Report on the U.S. Fish and Wildlife Service's Financial Statements for Fiscal Year 2000 (June 2001).
- ➤ Report: Department of the Interior Activities to Collect, Review, and Use Information That Identifies Individuals Who Access the Department's Internet Sites (April 2001).
- ➤ Audit Report: Personnel and Payroll Processing Policies and Procedures, National Business Center/Products and Services, Office of the Secretary, Department of the Interior (January 2001).
- Advisory Letter: The Collections Module of the Collections and Billing System, Bureau of Land Management (December 2000).
- ➤ OSM FY 2001 Financial Statement Audit Management Letter, Audit conducted by KPMG.
- ➤ BLM FY 2001 Financial Statement Audit Management Letter, Audit conducted by KPMG.
- > FWS FY 2001 Financial Statement Audit Management Letter, Audit conducted by KPMG.
- Notification of Findings and Recommendations issued by KPMG during the FY 2001 Financial Statement Audit of the Bureaus and Departmental Offices.
- ➤ Notification of Findings and Recommendations preliminary issued by KPMG for the FY 2002 Financial Statement Audit of the Bureau of Indian Affairs and Minerals Management Service.
- > Summary from DOI Homeland Security Assessment #2 -- an evaluation of the national critical infrastructure systems (July 2002).

General Accounting Office

- ➤ Audit Report: Information Security: Additional Actions Needed to Fully Implement Reform Legislation (May 2002).
- > Testimony: Information Security: Comments on the Proposed Federal Information Security Management Act of 2002 (May 2002).
- > Testimony: Financial Management: Effective Implementation of FFMIA is Key to Proving Reliable, Useful, and Timely Data (June 2002).
- > Testimony: Critical Infrastructure Protection: Significant Challenges in Safeguarding Government and Privately Controlled Systems from Computer-Based Attacks (September 2001).
- Audit Report: Information Security: Weak Controls Place Interior's Financial and Other Data at Risk (July 2001).
- ➤ Audit Report: Department of the Interior: Status of Achieving Key Outcomes and Addressing Major Management Challenges (June 2001).
- Audit Report: BLM's Actions to Improve Information Technology Management (February 2001).

APPENDIX 2

Department of the Interior

- > DOI Fiscal Year 2001 Annual Departmental Report on Accountability
- ➤ DOI Fiscal Year 2000 Annual Departmental Report on Accountability
- > DOI Fiscal Year 1998 Annual Departmental Report on Accountability
- DOI Fiscal Year 1997 Annual Departmental Report on Accountability
- DOI Fiscal Year 1996 Annual Departmental Report on Accountability
- DOI Fiscal Year 1995 Annual Departmental Report on Accountability

Office of Management and Budget

- ➤ Fiscal Year 2001 Report to Congress on Federal Government Information Security Reform
- OMB Analysis of Interior's 2001 Government Information Security Reform Act Report

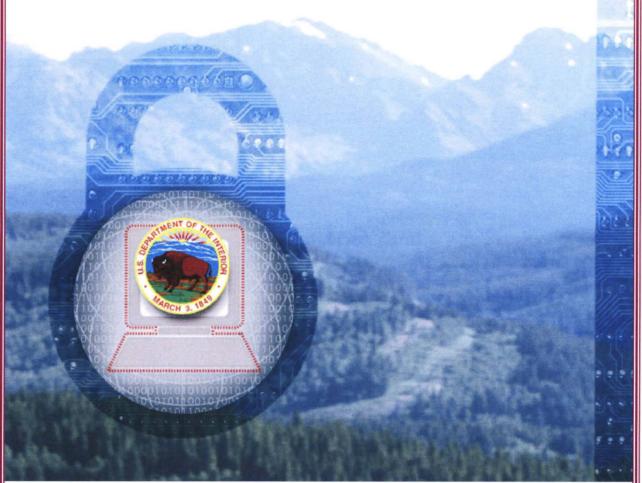
Other

- ➤ "SAS No. 70 Report for FSTN, Inc., on SEI Investments' Controls and Tests of Operating Effectiveness for TRUST 3000, SMAC, Trade 3000, INVEST 3000, and EBR, for the period November 1, 2000 through October 31, 2001 and StrataWeb for the period May 1, 2001 through October 31, 2001" conducted by PriceWaterhouseCoopers (November 2001). (SEI is a service provider for the Office of the Special Trustee for American Indians.)
- ➤ "Agreed-Upon Procedures Report on the Division of Payment Management, Program Support Center, Department of Health and Human Services, for fiscal year ending September 30, 2000," conducted by Ernst & Young (April 2001). (Department of Health and Human Services is a service provider for the government grant disbursements.)
- SAS No. 70 Report for FSTN, Inc., on SEI Investments' Controls and Tests of Operating Effectiveness for TRUST 3000, SMAC, Trade 3000, INVEST 3000, and EBR, for the period November 1, 1999 through October 31, 2000" conducted by PriceWaterhouseCoopers (November 2000). (SEI is a service provider for the Office of the Special Trustee for American Indians.)
- ➤ "Report on Controls Placed in Operations and Test of Operating Effectiveness, Federal Financial System, Department of the Interior National Business Center Enterprise Data Services Center for the period January 1, 2000 to September 30, 2000," conducted by KPMG (December 2000).
- Final DOI Initial Risk Assessment for Indian Trust Management (ITM) Systems (January 2002).
- ➤ NIST Computer Security Expert Assist Team (CSEAT) Review: High-risk Program Review Results For the Indian Trust Management Program (April 2002).

U.S. DEPARTMENT OF THE INTERIOR OFFICE OF INSPECTOR GENERAL

AUDIT REPORT

IMPROVEMENTS NEEDED IN
MANAGING INFORMATION TECHNOLOGY
SYSTEM SECURITY
NATIONAL PARK SERVICE



Graphic Courtesy of the U.S. Department of the Interior Office of the Chief Information Officer

REPORT NO. A-IN-NPS-0074-2003

MARCH 2004



United States Department of the Interior

Office of Inspector General

National Information Systems Office 134 Union Boulevard, Suite 510 Lakewood, Colorado 80228

March 29, 2004

To: Director, National Park Service

From:

Diann Sandy Wiann Sandy Manager, National Information Systems Office

Subject: Final Report, Improvements Needed in Managing Information Technology System

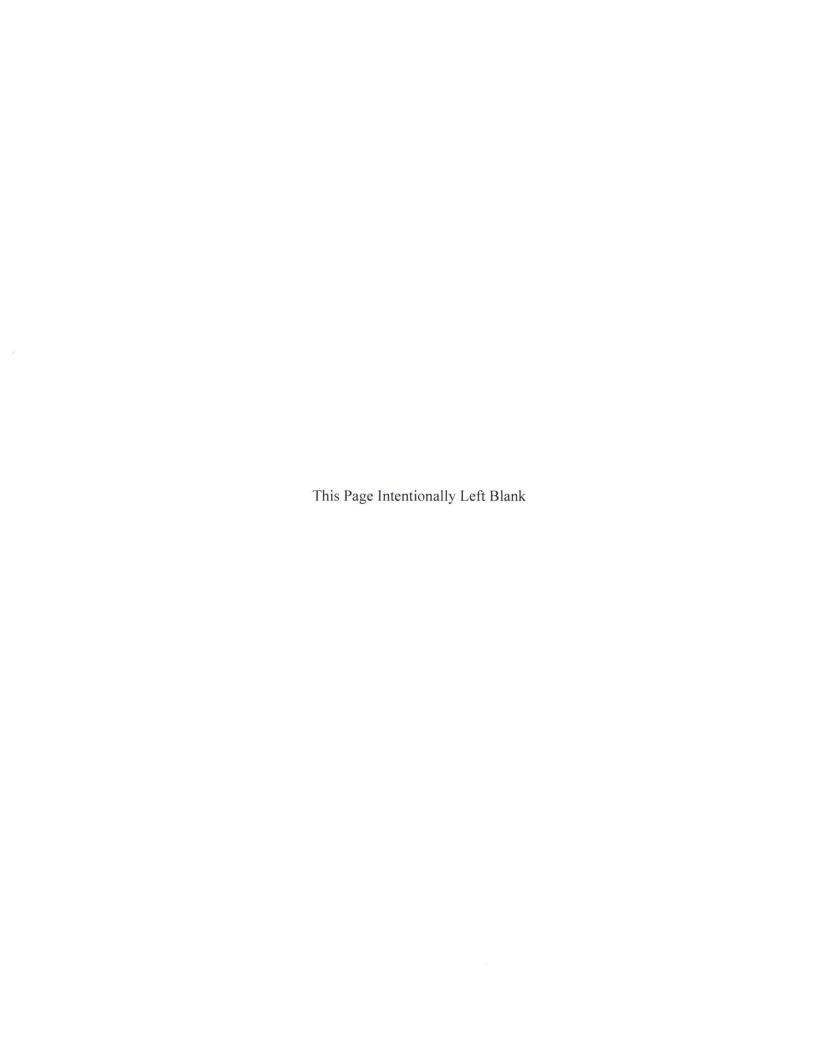
Security, National Park Service (No. A-IN-NPS-0074-2003)

The subject report presents the results of our audit of security over National Park Service's (NPS) information technology (IT) systems. The purpose of the audit was to determine whether controls effectively safeguarded the systems' integrity, confidentiality, and availability. Although NPS has recently improved the security of its IT systems, much remains to be accomplished before an effective IT security management program is implemented.

In the February 6, 2004 response to the draft report, the Director of NPS concurred with the report's 18 recommendations. Based on the actions described in the response and subsequent information provided by the Chief Information Officer for NPS, we classified 2 recommendations as resolved, 2 recommendations as resolved but not implemented, 10 recommendations as management concurs but additional information needed, and 4 recommendations as unresolved. The status of all the recommendations and the additional information requested is presented in Appendix 4.

The legislation, as amended, creating the Office of Inspector General requires that we report to the Congress semiannually on all audit reports issued, actions taken to implement our audit recommendations, and recommendations that have not been implemented.

Please provide a written response to this report by May 14, 2004. The response should supply the information requested in Appendix 4. We appreciate the cooperation provided by NPS staff during our audit. If you have any questions regarding this report, please call me at (303) 236-9243.



EXECUTIVE SUMMARY

BACKGROUND AND OBJECTIVE

To support its mission, the National Park Service (NPS) implemented local area networks in most of its approximate 400 offices, program centers, regions and support offices, and park units throughout the United States and its territories. These local area networks connect to 13 regional networks and one NPS-wide network. During our review, NPS reported to the Department of the Interior that NPS' major IT systems comprised 14 general support systems (networks) and 6 major applications. NPS established a senior executive service level chief information officer (CIO) position to provide standardized IT system security policy and management and to head the Office of the Chief Information Officer (OCIO). This office contains approximately 75 federal and contractor employees whose responsibilities included management of IT security and operation of three primary data centers located in Washington, D.C., and Denver, CO. NPS had also established information officers and IT security managers in program centers and regional offices to promote information and IT system security.

The objective of the audit was to evaluate the effectiveness of the management and controls over NPS' IT resources for ensuring integrity, confidentiality, and availability of information and IT systems. During our audit, we visited NPS locations as identified in Appendix 1.

RESULTS IN BRIEF

Despite recent organizational changes, we concluded that NPS lacked the basic foundation for an effective IT security program to ensure that issued IT security directives were consistently practiced. Specifically, NPS had not made sure that:

Personnel were empowered to fulfill their assigned IT responsibilities or were effectively evaluated; IT duties were separated; IT security duties and responsibilities were included in position descriptions; risks of performing IT functions were mitigated through appropriate assignment of position sensitivity levels and subsequent background clearances; and IT personnel were adequately trained to fulfill their duties and responsibilities.

- Information and IT system risks were effectively managed by: conducting asset valuations to properly categorize systems as mission critical, conducting adequate assessments of risks, and developing system security plans and Plans of Actions and Milestones.
- Technical and physical access controls were effectively managed and safeguarded personnel and IT resources.
- Changes to operating systems and applications were authorized, tested, and approved.
- ➤ IT services could be continued in the event of a system failure or disaster.
- ➤ IT security controls were integrated throughout NPS including incident response capability and a standardized network security infrastructure.

As a result, NPS information and IT systems are vulnerable to unauthorized access, misuse, and disruption of service and its IT resources are at risk of being unreliable.

RECOMMENDATIONS

We made 18 recommendations to improve the NPS information security program.

AGENCY RESPONSE AND OFFICE OF INSPECTOR GENERAL REPLY In the February 6, 2004 response to the draft report, the NPS Director concurred with the 18 recommendations. Based on the response and subsequent information provided, we considered 2 recommendations resolved and implemented, and classified 2 as resolved but not implemented, 10 as management concurs with additional information required, and 4 as unresolved. We requested that NPS provide us additional information on the unresolved recommendations.

TABLE OF CONTENTS

RES	ULTS OF AUDIT	1
	COMMENDATIONS FOR IMPROVING NPS' INFORMATION URITY MANAGEMENT PROGRAM	
	ENCY RESPONSE AND OFFICE OF INSPECTOR	21
	OIT OBJECTIVE, SCOPE, AND METHODOLOGY	
APP	ENDICES	
	SITES VISITED AND SYSTEMS REVIEWED SUGGESTED MATRIX OF POSITION SENSITIVITY DESIGNATIONS	
2	FOR A GENERAL SUPPORT SYSTEM	
	STATUS OF AUDIT REPORT RECOMMENDATIONS	

This Page Intentionally Left Blank

RESULTS OF AUDIT

NPS' organization does not support an effective information security management program. Until the National Park Service (NPS) implements a sound and consistently practiced information security program, it will have little assurance that its information technology (IT) systems provide reliable, confidential, and available information. An effective information security program should provide for assigning responsibilities, establishing and enforcing security policies and procedures, managing risk, and monitoring the adequacy of IT security controls. NPS has not, however, established the basic framework for a good program. As a first step, NPS needs to make IT security an overall top priority and ensure that all levels of management understand their roles and responsibilities and are held accountable for safeguarding information and IT systems. The discussions that follow highlight areas where we believe improvements are needed for NPS to have effective information security management program.

CIO lacked authority to be fully effective.

The NPS chief information officer (CIO) does not have the authority to manage all NPS information resources. Although the CIO position reports to a NPS Deputy Director, the CIO position has not been empowered to fulfill the responsibilities of a chief information officer. For example, the CIO is not an active member of the NPS National Leadership Council, as required by the Secretary of the Interior. As such, the CIO was not able to effectively aid senior management in identifying IT security requirements and in developing sound IT security strategies. We also found that although the CIO may develop IT security policies, procedures, standards, and guidelines, the CIO lacked the authority to issue and to enforce compliance with these IT security directives by office, program center, region, and park unit management. Figure 1 presents our understanding of NPS' IT management structure and shows that the CIO does not have authority over office, program center, region, and park unit IT staffs.

¹ The NPS National Leadership Council is the NPS' executive-level decision-making team. Secretarial Order, 3244, requires each bureau to have its CIO be a fully participating member of each bureau's executive leadership/management team.

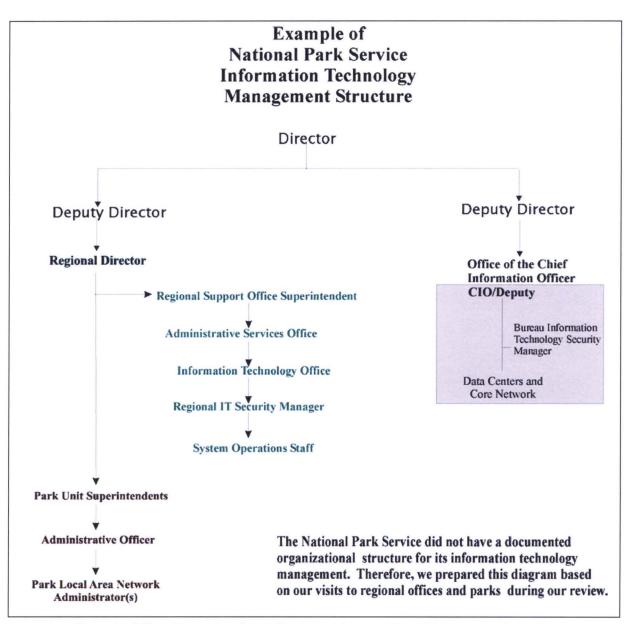


Figure 1. Office of Inspector General's representation of NPS' IT management structure.

Regional IT security managers lacked authority to be effective. Regional IT Security Managers (RITSM) were not delegated sufficient authority to exercise their responsibilities and were not at organizational levels commensurate with their IT security responsibilities. (See Figure 1 above.) In the two regions we visited, one RITSM was organizationally three levels below the regional director and the other RITSM was one level below the regional director. Also, one of the RITSMs stated he/she did not have the authority to enforce information security policies and procedures at the park units. We believe that the regional IT security function should be part of the regional directorate to be at an organizational level to exercise their responsibilities and authority.

Adequate separation of IT duties was not implemented throughout NPS.

NPS did not assign IT duties and responsibilities to provide for adequate separation of duties to prevent overriding critical processes by a single individual. For example:

- ➤ The Bureau IT Security Manager (BITSM) was responsible for overall NPS information security and was also designated the system security manager for the NPS primary wide area network, NPSNet. Therefore, the BITSM was responsible for reviewing his own activities. Additionally, the BITSM was performing as both the BITSM and as the OCIO Project Manager.
- ➤ RITSMs were responsible for IT security and performed daily regional IT operations. Therefore, they could not independently perform their security responsibilities.
- ➤ Individuals responsible for system security management were also responsible for administering systems and networks. For example, at the Network Management Office, Intermountain Region support office, Natural Resources Program Center, Rocky Mountain National Park, Point Reyes National Seashore, and Bandelier National Monument, system administrators were also performing IT security functions.
- At three data centers, application programmers had access to the data centers, which may provide programmers the opportunity to modify or change production data, operating system configuration, and database management systems. Generally accepted information security practices recommend that application programmers should not have access to production data, operating systems, and database management systems because of the risk that inappropriate or malicious code could be installed and result in a compromise of the information and IT systems.

We realize that separation of duties may not be feasible at each park unit, but controls could be implemented such that regional IT staff help support the park units by performing some of the park unit's security functions, such as reviewing system generated logs. At locations where adequate separation of duties cannot be achieved, NPS should ensure that risk assessments identify the lack of adequate separation of duties so that management understands this risk and can make a cost-effective decision to either mitigate or accept the risk.

Position descriptions and performance standards did not address IT security. Position descriptions for personnel with significant information security responsibilities, such as system owners, system and network administrators, and RITSMs, did not specify IT security responsibilities and duties. In addition, the CIO's performance standards did not include information security as a rating factor. Consequently, NPS management and personnel that should be responsible for ensuring IT resources are adequately safeguarded could not be evaluated based on how they performed their security responsibilities.

Level of risk associated with IT positions was not established. NPS had not established an overall sensitivity level for IT positions in relation to the duties to be performed. The Departmental Manual (441 DM 3) requires that positions be reviewed to determine the risk of an individual performing the duties of the position and for assigning the appropriate sensitivity level for those positions. Specifically, NPS had not designated the appropriate sensitivity level of public trust² IT positions, such as system security manager, system administrator, and telecommunications specialist, commensurate with the risks associated with the duties. For example:

- Position sensitivity designations were different for personnel performing the same IT duties. One RITSM was designated a sensitivity level of "non-sensitive" (low risk), while the other was designated a sensitivity level of "noncritical-sensitive" (moderate risk). This resulted in NPS management accepting different levels of risk for positions with similar duties and functions. In addition, different types of background investigations would be required.
- ➤ IT positions and functions being performed by contractors were not assigned sensitivity levels. For instance, we reviewed three contracts that provided for contractor personnel to perform IT functions at NPS' data centers. We found that the contracts had no requirement for designating sensitivity of the contractor positions, such as application programmer, network administration, and telecommunications support, or for background investigations and resultant security clearances. One of these contracts required contract employees to be fingerprinted and for background checks to be performed. However, NPS was not able to substantiate that background investigations were completed and that the appropriate security clearances were obtained.

4

² According to the Departmental Manual (441 DM 3), public trust positions are those that are not related to national security duties.

Management at one region stated that background reinvestigations had not been performed of its employees.

To determine position sensitivity, NPS could develop a matrix of all positions related to IT responsibilities and identify the associated risks to information and IT systems and the sensitivity level of those positions. Appendix 2 presents an example of this matrix concept.

IT training required to safeguard IT resources was not mandated.

During our site visits throughout NPS, we observed that overall the IT staffs at these sites were resourceful and effective in providing IT services and customer support. However, while NPS provided basic computer security awareness training and other IT-related training, it did not ensure that IT specialists in regions and park units were encouraged or required to receive training specific to information security and IT security management. For example, an IT specialist at a park unit had to determine on his/her own how to implement a new system. In addition, at most locations we visited, personnel had not been provided training specific to their duties and fulfilling their responsibilities in managing and operating NPS networks and servers. For instance, one IT specialist did not receive training on implementing a planned new NPS operating system. In that regard, NPS had not developed an IT career management program that included training requirements for all levels of IT positions. Without a structured training program for employees with IT responsibilities, NPS lacks assurance that networks, systems, and data were adequately safeguarded.

IT systems were not properly categorized.

NPS did not properly categorize its general support systems and applications as mission critical. The Department of the Interior's "Asset Valuation Guide" requires bureaus to categorize an IT system that processes, stores, or transports (1) Privacy Act or proprietary information as Mission Critical and (2) financial-related information as Financial Systems, which is above mission critical. The guideline also states that IT systems that are critical to the support of the Department's core missions and goals and not assigned a higher category are to be categorized as mission critical. Almost all NPS networks transport these types of information; however, NPS categorized its networks at a lower level—business essential. Further, NPS' Facilities Maintenance Support System, a major application, was categorized as business essential, even though the information in this system was used and maintained to support a DOI mission goal. Without performing asset valuations to properly categorize its systems, NPS has little assurance that all system resources have appropriate levels of protection.

IT risk assessments were not performed.

NPS had not performed risk assessments for 17 of its 20 general support systems and major applications. NPS reported to the Department that risk assessments had been performed for the 3

remaining systems—a general support system (NPSNet) and 2 major applications (Lotus Notes/Domino and ParkNet). However, we reviewed two of these risk assessments (NPSNet and Lotus Notes/Domino) and found that the assessments were incomplete, as follows:

- ➤ The NPSNet risk assessment was an initial assessment, which is less detailed and less extensive than a full risk assessment.
- The Lotus Notes/Domino risk assessment focused only on three major data centers, which would not likely represent the NPS-wide risk environment. Also, the assessment did not identify and assess all possible risks such as those introduced by the supporting general support systems. Further, the assessment was based on the loss of operations only, and did not consider the value of the data maintained in the major application.
- Neither of the risk assessments included:
 - Input from all data owners, such as program center managers, regional directors, or park unit superintendents, in the determination of the risks.
 - Evidence that management agreed to mitigate the identified risks or to accept the residual risks.

Therefore, the level of risk may not be at an acceptable level to ensure that all information processed, stored, and transported was adequately safeguarded and that residual risk was understood and accepted by management.

System security plans were not adequate.

NPS began drafting system security plans for local area and wide area networks, such as NPSNet, Intermountain Region,³ Pacific West Region, and Natural Resources Program Center networks. This is good; however, the requirement for system security plans was established in 1987.⁴ The purpose of a system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. System security plans should include the elements identified in the National Institute of Standards and Technology

³ Intermountain Regionwide area network security plan included appendices for 67 of the park units within the region.

⁴ Computer Security Act of 1987 required that for each system a plan for the security and privacy of each Federal computer system be developed one year after the enactment of the Act.

Special Publication 800-18 "Guide for Developing Security Plans for Information Technology Systems," and DOI policies. However, the NPS security plans did not always include the following required features:

- > Appropriate assignment of responsibilities.
- Appropriate classification of data sensitivity and criticality that was processed, stored, and transported.
- Descriptions of components of general support systems and the applications they support.
- Identification of general support systems that support the major applications.
- ➤ Identification of all of the interconnection points (including Internet service providers and dial-in access) and agreements for connecting to other NPS internal and external networks.
- > Physical and environmental controls.
- ➤ All milestone dates for implementing planned controls.

In a related matter, the CIO was in the process of consolidating individual park unit local area networks and regional wide area networks for the purpose of performing only one certification and accreditation. Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Resources" stipulates that any interconnected system, such as a local area network, under the same direct management control is considered a general support system requiring a system security plan. Local area networks at the park units and the regions are under the management control of the park superintendents and the regional directors, respectively. Therefore, we believe that unless the consolidated system is under the direct management control of the CIO, each network will require a separate security plan that should be included as part of the one general support system security plan.

Plans of Actions and Milestones were not adequate. OMB requires that agencies develop Plans of Actions and Milestones (POA&M) for every program and system for which weaknesses are identified through internal and external reviews. The POA&M process is to aid management in identifying, prioritizing, and monitoring the progress towards correcting the security weaknesses. Although NPS' POA&Ms have improved, they were not adequate for the following reasons:

- All of the weaknesses identified by the Office of Inspector General (OIG), NPS internal control reviews, and DOI program reviews were not included. For example, all financial statement findings related to IT that had been reported by the OIG for fiscal years 2001 and 2002 were not included in the POA&M.
- ➤ There was no prioritization or strategy for correcting the weaknesses. For example, a security plan was to be developed for a general support system by July 1, 2003, whereas prerequisite reviews and documents, such as an asset valuation, a technical vulnerability assessment, and a management control review, were not planned to be completed until October 1, 2004.
- Dates reported for corrective actions were not consistent with the supporting documentation. For example, in the June 2003 POA&M submitted to the Department, NPS reported that the system security plan for NPSNet was completed in December 2002; however, only a draft system security plan dated June 2003 had been done.
- All of the weaknesses in systems' components were not identified by NPS and therefore were not included in the POA&M. For example, NPS did not recognize that storing backup media at employees' homes was a security weakness.
- ➤ Incremental steps needed to mitigate identified weaknesses were not reported. For example, in the June 2003 POA&M, NPS identified a weakness related to Internet connections. The planned corrective action involved two options and one milestone completion date of December 30, 2004. However, the POA&M did not include steps and completion dates for determining which option to select and the incremental steps for implementing the selected option. Consequently, NPS reported the status of this particular item action as "ongoing" and did not indicate the progress in correcting the weakness.

During the course of our audit, NPS began to identify the resources needed to correct the reported IT weaknesses. However, these resource costs had not been integrated with the NPS IT capital planning and control process.

System users' accounts were mismanaged throughout NPS.

Because system users' accounts were managed by each NPS organizational unit (offices, program centers, regions, and park units) and inconsistent methodologies were practiced in managing system user accounts, NPS had little assurance that users' access

levels were based on the users' day-to-day activities or that the user accounts were authorized. For example:

- ➤ User accounts were not always disabled or deleted when individuals left NPS or changed positions within NPS.
- Users were issued multiple system user identifications, which may allow them to circumvent system access controls and bypass separation of duties.
- ➤ Users at one park unit were automatically provided dial-in access when their user accounts were established by the park unit's IT staff even though we found no evidence that the users were authorized this type of access.
- There appeared to be no periodic review of user accounts by system owners or supervisors to ensure that the level of access granted was appropriate for each system user.

Password management was inconsistent.

NPS had not consistently applied standard password procedures and practices for its servers to ensure adequate password management. For example, at one location the setting for lockout duration was "Forever" and at another location the setting was for 90 minutes. If the setting for "password lockout duration" is not set on "Forever" an intruder has the opportunity to obtain the password because it allows unlimited guesses. Additionally, we found that password settings in servers at some locations allowed users to circumvent the requirement for changing their passwords periodically. Consequently, the users could continually change their passwords until their original password could be used again. As a result, NPS systems may be operating with less stringent controls than expected by management.

Physical access to IT resources was not sufficiently controlled and monitored.

We found that access to data centers was not always adequately controlled. For example:

Although the Information Technology Center (ITC) used access cards and video monitoring as physical access controls to the data center, individuals who had key cards and accessed the data center were not always approved for access. We also noted that there were an excessive number of personnel with access to the data center, such as application programmers who were not part of the ITC or the OCIO. Due to potential blind spots in video monitoring, best practices suggests that methods be used to monitor personnel exiting data centers.

At the National Information Systems Center (NISC) data center, access was through the use of a cipher door lock. Although there were sign in/sign out logs, only non-NISC personnel were required to sign the logs. Consequently, there was no record of NISC personnel activities and specific NISC personnel could not be held accountable for any misuse of computer resources.

At the park units we found that:

- Access to telecommunications closets was not limited. That is, they were located in general working areas, such as where a copy machine was located, a loading/receiving dock, a break room, and an amphitheater.
- ➤ One server room was located in a general work area and was accessible by personnel other than IT personnel.

Environmental controls were not adequate to protect personnel and IT equipment.

At many park units visited, we noted that the server rooms did not adequately protect personnel and IT equipment. Specifically, some server rooms did not have adequate air conditioning units and proper fire suppression capabilities. For example, at Bandelier National Monument:

- The air conditioner in the server room had a water leak. Although a bucket was placed below the air conditioner to catch the water, we observed water stains on the floor.
- Access to the server room was from the outside of the building and the access door was not sealed, thus the room was susceptible to dust, sand, and rain.

The room was too small to house all of the equipment along with personnel and to provide for proper wire management. See Figure 2.





Figure 2. Photographs of the Bandelier National Monument Server Room

Although many park units use historical buildings as facilities for housing local area network server rooms, locating servers in historical buildings should not preclude NPS from implementing adequate environmental controls. Some examples of improvement that would not require changes to the historical structure or the building of new facilities may include:

- Installing air conditioning units.
- Installing rack and shelf systems to better use small spaces.
- Installing weather seals around doors.
- Supplying fire extinguishers.

Change management controls were not effective.

NPS has an Information System Life Cycle Manual which contains instructions on managing changes to systems. However, NPS did not have adequate controls over changes to computer hardware, such as computers, servers, and routers; operating systems; and application software. We found no evidence that changes made by IT personnel in program centers, regions, and park units to operating systems and application programs were authorized, tested, and approved prior to installation. We also found no evidence that the program centers, regions, and park units were required to develop test plans for changes and enhancements to operating systems and application software.

Continuity of services planning needs improvement.

NPS has not instituted adequate continuity of services planning. Continuity of services planning helps management identify and prioritize those daily processes or critical business functions that need to be restored first after emergencies, such as power interruptions or system failure. Weaknesses we observed in NPS' preparation for continuity of services included:

- Inadequate backup practices and offsite storage facilities to keep backup media and system and application documentation. For example, NPS practices did not include full back up of data and systems on any scheduled cycle.
- Using employee homes as the off-site storage location for application software and network operating system backup media rather than a location that could be easily accessed by all required personnel.
- Not storing at an off-site location security documents, such as system security plans and continuity of operations plans.
- Not testing those contingency or continuity of operations plans that did exist.

Incident response capability was not fully developed.

While some guidance had been issued, NPS had not distributed specific procedures for incident detection, reporting to FedCIRC. and responding to incidents. Additionally, we believe NPS' policy for computer incident response was insufficient because it did not: (1) include all types of incidents, such as the misuse of government computers; (2) provide the protocol for communicating an incident; and (3) specify the procedures for mitigating an incident. For example, one regional network manager reported to the NPS wide area network management that an Internet scan had occurred of the regional network, which was trafficked through the NPS wide area network firewall. However, the regional network manager did not receive feedback or a response from NPS management, thus the regional network manager had little assurance that the potential incident had been mitigated. In addition, NPS had not ensured that all individuals responsible for IT security management were adequately trained in their incident handling responsibilities.

Capability for detecting, identifying, and reporting IT misuse was limited.

NPS was not routinely creating, reviewing, and maintaining system logs for network operating systems and routers. System logs are used to detect and identify system misuse or inappropriate actions of authorized and unauthorized users. At several locations the logs were set to overwrite at a very low threshold; thus the logs were overwritten frequently and historical information was

lost. At some locations we visited, the logs were not created, and logs that did exist were not being periodically reviewed. NPS had no policy for creating, reviewing, and maintaining system logs. Without appropriate logging of system activities, NPS may not be aware of potential incidents and be able to timely identify individuals who were misusing IT resources.

Standardized configuration of network security infrastructure was lacking.

There was no standard configuration of NPS' network security infrastructure, such as the use and placement of firewalls and intrusion detection systems. At one park, IT security personnel incorrectly assumed that the NPS wide area network, NPSNet, was providing security to protect their specific network, systems, and data. We also found that regions and park units had not always implemented significant protection for their networks such as firewalls. At two locations that had implemented firewalls, IT system administrators detected scanning of their networks from the Internet, which could be considered a threat that was not blocked at the NPSNet level. Without a standard security configuration, NPS was not able to effectively protect its IT resources and ultimately implement security best practices.

RECOMMENDATIONS FOR IMPROVING NPS' INFORMATION SECURITY MANAGEMENT PROGRAM

We recommend that the Director, NPS:

- 1. Assign to the CIO the duties and responsibilities as defined by the Secretary and authorize the CIO to issue information security directives to NPS personnel with IT security responsibilities.
- 2. Implement an effective information security program. In establishing this program, NPS should consider:
 - Dual reporting of information security management staff:
 - At regions, RITSMs should report to the regional directors and to the CIO and be authorized to carry out IT security management responsibilities directly to regional and park IT staff.
 - At park units, IT personnel should report to the superintendents and to the regional information security managers.
 - Dedicate the BITSM and RITSMs to only security program management.
- 3. Provide written notification to personnel with IT security responsibilities specifying their duties and functions. Hold individuals accountable for fulfilling these responsibilities through annual performance evaluations. In meeting this requirement, NPS should:
 - Identify all individuals/positions such as associate directors, program managers, regional directors and all staff who are responsible for managing and administering NPS IT systems, networks, and data.
 - Review position descriptions of all positions identified as having IT security responsibilities and update the position descriptions to reflect current duties and responsibilities.
 - Update individual performance evaluation plans for those positions identified as having IT security responsibilities to include information security management tasks, functions, and strategic planning.

- Designate, for each position having IT responsibilities, a sensitivity level commensurate with the risks of the duties performed and ensure the appropriate background checks or rechecks be performed based on the designated sensitivity level.
- 4. Separate the duties and responsibilities of IT personnel to ensure that unauthorized activities can be detected timely. To ensure duties and responsibilities are adequately separated NPS should:
 - ❖ Identify personnel at all locations who have IT security management duties and responsibilities and who are also responsible for performing system and network administration duties. If possible, separate these duties or develop alternative processes to provide for separation of duties.
 - Implement alternative controls, such as, moving some security management responsibilities to different organizational levels if separation of duties at some locations is not cost effective.
 - Identify personnel at all major data centers who are responsible for programming software applications and for system administration functions and separate these duties or develop alternative processes to provide for separation of duties.
 - ❖ Identify the lack of separation of duties in the security plans and require management to formally accept the risk associated with the lack of separation of duties if alternative controls are not feasible.
- 5. Modify all IT support contracts to require position sensitivity for all IT positions and require appropriate background investigations and security clearances for all contractor personnel performing IT functions.
- 6. Establish an IT career-training program for all NPS IT professionals. The training program should be based on NPS' implemented and planned systems, networks, and software. NPS should periodically review the training program to ensure that IT professionals are provided training on the most current security requirements and the most up-to-date technology implemented or planned by NPS.
- 7. Perform asset valuations for all general support systems and applications to properly categorize these systems based on their importance and critical loss criteria in accordance with the Department's "Asset Valuation Guide."
- 8. Perform risk assessments of all general support systems and major applications to identify risk, threats, and vulnerabilities that impact the accomplishment of the NPS' and the Department's missions and the

security and data integrity, confidentiality, and availability. NPS should also ensure that risk assessments include input from senior management and data owners.

- 9. Develop security plans for all general support systems and major applications following NIST and Departmental guidelines.
- 10. Establish procedures to ensure that the POA&Ms are used as a management tool. The procedures should include:
 - Requirements for reporting all the weaknesses identified and reported by OIG, NPS, and other reviews performed on behalf of NPS.
 - ❖ A prioritized strategy to correct all identified security problems.
 - Assurance that the completion dates are supported by the applicable documentation.
 - Requirements for corrective actions that exceed 6 months to have incremental steps to correct the weaknesses, milestone dates, and resources required.
 - Integration of resources identified in the POA&Ms for correcting weaknesses with the capital investment planning and control process.
- 11. Establish a standardized process for system user accounts that includes:
 - ❖ Coordinating with Human Resources, system owners, and supervisors to identify and report to the IT system security administration staff the names of employees who are no longer employed by NPS, have a change in responsibilities and duties, or have transferred from NPS locations. Upon notification, IT system security administration staff should disable user accounts or immediately terminate access from all applicable systems, applications, and data centers.
 - ❖ Establishing a policy requiring each user of NPS systems to have unique user identifications. The policy should specifically state when a single user could have multiple identifications and describe the controls to ensure the use of multiple identification does not circumvent separation of duties.
 - Developing procedures requiring system owners or supervisors to periodically review and validate users' access and privileges.

- 12. Establish standard password configuration settings to ensure that all IT system resources are protected at an acceptable level.
- 13. Establish policies, procedures, and practices to ensure that physical and environmental controls protect systems and data from misuse or interruption, and physical damage or destruction and that personnel have a safe working environment. In developing these policies, procedures, and practices NPS should:
 - Evaluate the facilities that house the data centers, server rooms, and telecommunications closets to determine if the access controls and environmental controls are effective. If the controls are not effective, identify cost effective remediation controls and report the status in NPS' POA&Ms.
 - * Review the current lists of personnel with access to the all data centers and determine if the access granted is necessary and revoke access that is not required.
 - Require the use of sign in/sign out logs or other entrance/exit technologies at data centers and compare physical access logs to computer logs.
- 14. Establish standard change management procedures to ensure that all changes are authorized, tested, and approved prior to updating operating systems and applications. To aid in standardizing its change management process, NPS should consider the use of change management software to assist in the control over modifications made to operating systems and applications.
- 15. Establish policies and procedures to ensure that all NPS systems and applications can be restored or recovered timely in the event of system failures or disasters. These policies and procedures should:
 - Define the appropriate backup and recovery requirements of IT services that clearly define personnel roles and responsibilities and standard types of back-ups and timeframes for backing up systems and data.
 - Define appropriate offsite storage locations and ensure that backup data and system documentation are stored in these offsite storage locations.
 - Develop continuity of operations plans for all NPS locations and ensure that the plans are tested and updated annually.

- 16. Establish an incident handling organizational structure and a process for identifying, reporting, and mitigating computer-related incidents.
- 17. Establish policies and procedures to ensure that systems are logging relevant information, logs are maintained for an appropriate period of time to provide an adequate audit trail of systems activities, and the logs are reviewed periodically to identify inappropriate activities.
- 18. Establish standard network security infrastructure based on a layered security approach that includes firewalls and intrusion detection systems throughout the NPS internal networks. To accomplish this layered security approach, NPS should:
 - * Require networks topologies be developed for all offices, program centers, regions, and park units to determine the appropriate security infrastructure solution that complies with best practices.
 - Create standard firewall rules that prevent unauthorized access from the Internet into the park unit networks.

AGENCY RESPONSE AND OFFICE OF INSPECTOR GENERAL REPLY

In the February 6, 2004 response to the draft report (Appendix 3) the NPS Director concurred with the 18 recommendations. The response described recent NPS IT security accomplishments, and commented on the findings and recommendations. Also, the NPS CIO provided subsequent information about the report and the response. We revised the report as we considered appropriate based on the NPS response and additional information provided.

Based upon NPS' replies, we classified Recommendations 7 and 8 as resolved; Recommendations 12 and 13 as resolved but not implemented; Recommendations 1, 2, 3, 4, 5, 6, 10, 11, 14, and 16 as management concurs but additional information required; and Recommendations 9, 15, 17, and 18 as unresolved. (See Appendix 4.) Even though NPS agreed with all the recommendations, we considered four of the recommendations as unresolved because the proposed actions did not meet the intent of the recommendations, as discussed below.

Recommendation 9. Although NPS completed all "initial" system security plans in December 2003, our recommendation was to develop system security plans for all general support systems following NIST Special Publication 800-18 and Departmental guidelines. While Departmental guidelines include the development of "initial" system security plans, these initial plans are not a finalized system security plan. That is, they do not include information from risk assessments and system testing and evaluations. As such, they do not adequately address the controls necessary to reduce risk to an acceptable level. Further, NPS disagreed that system security plans were needed for each park unit's and regional office's local area networks even though these networks are under the management control of the respective parks and regions. According to Office of Management and Budget Circular A-130, Appendix III, these networks are general support systems requiring system security plans. Furthermore, without system security plans for each of these local area networks, NPS has little assurance that these networks are operating securely and that the NPS-wide network is adequately safeguarded. NPS should prepare a plan for developing system security plans for all general support systems and major applications and for incorporating park units and regional office local area networks into its one general support system.

Recommendation 15. NPS stated that a continuity of operations plan would be completed by its IT Infrastructure team by 2005. Our

understanding is that NPS is developing one continuity of operations plan for its one general support system. If that is the case, we do not believe that NPS will have sufficient procedures to ensure that major applications are restored timely and those NPS locations that input, process, transport, and store information will be able to recover from system failures or disasters expeditiously. NPS should develop policies and procedures ensuring that NPS information, systems, and applications can be restored or recovered timely; that backup and recovery is practiced by all levels of NPS management; that offsite facilities are adequate; and that continuity of operations plans are tested and updated annually.

Recommendation 17. NPS is requesting funding for acquiring software to manage system events. Our recommendation, however, dealt with preparing policies and procedures to make sure relevant information about system events was logged and reviewed. As logging capability currently exists within most NPS systems, the intent of our recommendation was for NPS to consider acquiring a software tool that would take advantage of existing logging capability and for NPS to periodically review logs to identify inappropriate activities.

Recommendation 18. The response focused on the conversion of the NPS core networks to the Department's Enterprise Services Network. However, the recommendation was for NPS to develop a layered approach to security to include safeguarding all internal networks, such as the networks operated and maintained at regions and park units.

AUDIT OBJECTIVE, SCOPE, AND METHODOLOGY

Our objective was to evaluate the effectiveness of NPS' management and controls over IT resources to ensure integrity, confidentiality, and availability of information and IT systems. Specifically, we evaluated information security management practices and general controls over non-financial IT systems (see Appendix 1 for the systems reviewed).

To evaluate these controls, we reviewed NPS policies, procedures, and practices in place during April through August 2003, tested and observed security practices and IT security control techniques in operation, and held discussions with NPS staff to determine whether IT security controls were in place, adequately designed, and operating effectively. We performed on-site work at NPS headquarters in Washington, D.C. and other NPS locations listed in Appendix 1.

Our audit was conducted in accordance with the "Government Auditing Standards" as issued by the Comptroller General of the United States. Accordingly, we included tests and other auditing procedures that were considered necessary under the circumstances.

SITES VISITED AND SYSTEMS REVIEWED

Office of the Chief Information Officer

Network Management Office (NMO) NPS wide area network (WAN)/(NPSNet) Denver, Colorado

National Information Systems Center (NISC)

Denver, Colorado

Denver General Support System (GSS)/local

area network (LAN)

Information Technology Center (ITC)

ITC LAN

Washington, D.C.

Natural Resources Program

Natural Resources Program Center (NRPC)

NRPC GSS/LAN

Ft. Collins, Colorado and

Denver, Colorado

Intermountain Region (IMR)⁵

Santa Fe Support Office

IMR GSS/WAN

Santa Fe, New Mexico

Rocky Mountain National Park

Rocky Mountain LAN

Estes Park, Colorado

Bandelier National Monument

Bandelier LAN

Los Alamos, New Mexico

Pacific West Region (PWR)

Regional Office and Pacific Great Basin

Support Office PWR GSS/WAN Oakland, California

Golden Gate National Recreation Area

Golden Gate LAN

San Francisco, California

Point Reyes National Seashore

Point Reyes LAN

Point Reyes, California

⁵ The Intermountain Regional Office headquarters is located in Denver, Colorado and is supported by the National Information Systems Center. The Santa Fe Support Office provides support for regional and support personnel located in Santa Fe, New Mexico and for all the parks in the region.

SUGGESTED MATRIX OF POSITION SENSITIVITY DESIGNATIONS FOR A GENERAL SUPPORT SYSTEM

(The minimum level of investigation associated with Public Trust Positions)

Role	Position	Designation Investigation Requirement ⁶	Justification
Program Manager	Deputy Director	High Risk – BI	Senior manager for system. As program manager who has ultimate management authority for systems.
Information Owner	Program Managers, Regional Directors, Park Unit Superintendents	Moderate Risk – MBI	Senior manager for data contained in the system for their individual program, region, or park unit. System security and back-up procedures, minimize the opportunity for a regional director, superintendent or program manager to do major harm to the system. Oversight provided by headquarters.
Information System Owner	CIO	Moderate Risk – MBI	Minimal system access. Provides policy oversight for data management.
Security Manager	BITSM/RITSM	High Risk – BI	Responsible for system integrity, confidentiality, and availability. Prepares bureau policy for system security.
System Manager	Deputy CIO	High Risk – BI	Provides technical oversight to all system operations and administration from a headquarters level. Provides policy and guidance for regional and field operations.
System ⁷ Security Manager	Multiple employees located in headquarters, offices, program centers, regions, and park units.	Moderate Risk – MBI	Responsible for system security design, testing, and maintenance under the technical guidance of the OCIO.
System ² Administrator	Multiple employees located in headquarters, offices, program centers, regions, and park units.	Moderate Risk – MBI	Responsible for system operation and maintenance at headquarters, offices, program centers, regions, or park units. Work is under the technical oversight of Regional Directors or Associate Directors.
Internal NPS Users ²	Office, program center, regional, and park unit employees	Low risk – NACI	Responsible for data entry and update. Access to the system is limited to the functions performed and registration is required and managed by the system security managers or system administrators.

This matrix was developed by the Office of Inspector General for use by the National Park Service as a guide to develop position sensitivity designations consistently for its personnel with IT responsibilities. The matrix was based on a U.S. Geological Survey review of roles and positions identified with IT responsibilities for one of its major applications. For each role and position, a level of risk/sensitivity and the related type of background investigation was defined along with the justification for the sensitivity level and type of background investigation.

⁶ BI – Background Investigation; MBI – Minimum Background Investigation; NACI – National Agency Checks and Inquiries.

⁷ The duties and background investigation requirements are applicable to federal employees, contractor employees, and volunteers.



United States Department of the Interior

NATIONAL PARK SERVICE 1849 C Street, N.W. Washington, D.C. 20240

N REPLY REFER TO

S72(2550)

FEB - 6 2004

Memorandum

To:

Manager, National Information Systems Office

Office of Inspector General

From:

Director For P. Mall

Subject:

Response to Draft Report on Improvements in Managing Information

Technology System Security, National Park Service

(Assignment No.A-IN-NPS-0074-2003)

We appreciate your recent review of our Information Technology (IT) Security program. It offers us the opportunity to get an outside view of our strengths and weaknesses as well as suggestions for improving the National Park Service (NPS) in this area. We are certain the recommendations and other related comments provided by you and your staff will go a long way toward making the NPS IT stronger than ever.

In this memorandum and its attachments, the NPS addresses each of the findings and recommendations presented by the Office of Inspector General (OIG) in the report entitled *Improvements in Managing Information Technology System Security, National Park Service.* Appendix A contains comments directed to the findings and Appendix B contains comments on recommendations.

We have also provided some general comments regarding the audit in addition to our specific responses to the Findings and Recommendations.

Prior to my tenure, the NPS had no IT governance structure other than a single IT advisory council composed primarily of IT specialists. Most Servicewide initiatives were conducted by regions and program offices volunteering their resources. IT policies and procedures were virtually non-existent and each region and park managed their IT assets as they determined appropriate. Program areas managed their system development and implementation efforts in a decentralized, non-integrated manner. Few IT security measures had been implemented and the NPS did not have either a Chief Information Officer (CIO) or a Bureau IT Security Manager (BITSM).

FOR OFFICIAL USE ONLY

Many of the governing statutes and requirements have been in place for a number of years. Since July 2001, however, NPS has moved forward on a rapid pace to ensure its IT assets were properly managed and secured. We have highlighted, for the OIG's consideration, some of the significant improvements the NPS has made during the current administration as an indicator of the NPS' resolve to continue improving:

- The establishment of the CIO and BITSM positions
- The creation of NPS's first IT Investment Council
- Combined two separate NPS IT organizations into one under the direct control of the CIO.
- Successfully responding to DOI requirements for securing our network perimeter, including the installation of firewalls and intrusion detection software
- Movement of over 50 NPS web servers into a centrally managed DMZ
- The implementation of an IT asset management system that tracks every desktop in the NPS
- Authorization of the CIO to shut-down any system or IT infrastructure component failing to meet NPS security directives
- The development of an internal application to track systems, IT personnel, network components, recently expanded to include radio equipment
- The standardization of 13 general support systems (GSS) into one enclave
- The creation of configuration management boards for our wide-area-network (WAN), desktop and local-area-network (LAN) infrastructure, Active Directory (AD) and our voice systems; who are now constructing the standard Servicewide policies and procedures upon which sound operations can be based and will form the foundation of a strong IT security posture.
- The establishment of a formal NPS Computer Incident Response Team using the Regional IT Security Managers (RITSMs)
- The purchase of 500 computer-based on-line training licenses for its IT specialists in FY 2002 – 2003.
- NPS has purchased a policy and procedures template that may be used as both a model and a taxonomy for classifying policies.
- The creation of information officers, technology officers, regional IT security managers at each region and program office
- The issuance of a formal software development lifecycle handbook
- NPS is leading Departmental initiatives for applications in law enforcement and records management
- Playing a major role in the reservation module of the RecOneStop
- Taking a lead role in the Enterprise Services Network (ESN)
- Management of the NPS Active Directory implementation which is on schedule to meet the Department's December deadline
- Completing Interim approval to operate on all major applications

FOR OFFICIAL USE ONLY

- Meeting all FY 2003 Government Paperwork Elimination Act requirements
- Taking the lead in negotiating the Microsoft Enterprise Agreement which established the model for the Departmental agreement
- Using FY 2003 funding for new positions to add a second IT security staff member as an Associate BITSM and reassigning a third employee as a second Associate BITSM.
- Encouraging security credentials for our IT managers with NPS having the only CIO in DOI with not one, but two IT security certifications (Certified Information Systems Security Professional - CISSP and Global Information Assurance Certification Security Leadership Certificate – GLSC). In addition, our BITSM, Associate BITSM, Chief Technology Officer and a number of RITSMs have earned the CISSP credential. Our Deputy CIO for Systems has earned the Certified Information Systems Security Management Professional (CISSM).

We fully understand there is much work to be accomplished and NPS is far from satisfied. However, the process of developing an acceptable IT security framework rests on: 1) a strong IT governance platform with standard policies and procedures; 2) an organization that values a common approach to the management of its IT assets through compliance; and, 3) an organization that works internally as a team. We feel we are well on the way to establishing this solid base.

Most of the recommendations have significant budgetary implications and the result of implementing these recommendations will have a major impact on the operations of the NPS. We will actively work with the DOI and the Office of Budget and Management in an effort to identify funds for reprogramming in order to fully implement all the recommendations. The NPS will, with guidance from the Department, also continue to assess the value of our assets against the potential risks. There may be cases where we find that certain risk mitigation efforts are too costly when weighed against the risk probability, and, in these instances, we may decide to accept the risk.

For additional information, please contact the CIO, Dom Nessi at 202 354-2093.

Attachments

- A Comments on Findings
- B Comments on Recommendations
- cc: Assistant Secretary for Fish and Wildlife and Parks
 Audit Liaison Officer, Assistant Secretary for Fish and Wildlife and Parks
 Audit Liaison Officer, National Park Service
 Focus Leader, Management Accountability and Audit Follow-up

Attachments withheld by the Office of Inspector General.

- 3 -FOR OFFICIAL USE ONLY

STATUS OF AUDIT REPORT RECOMMENDATIONS

RECOMMENDATION REFERENCE	STATUS	ACTION REQUIRED
7 and 8	Resolved	No further response is required.
12 and 13	Resolved, not implemented	No further response to the Office of Inspector General is required. The recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
2, 3, 4, 6, 10, 11, and 16	Management concurs, additional information required.	Provide the title of the official responsible for implementation.
1, 5, and 14	Management concurs, additional information required.	Determine how the recommendation will be implemented and provide plans describing implementing actions, target dates, and responsible officials
9, 15, 17, and 18	Unresolved.	Reconsider the proposed corrective actions and provide an updated reply.



U. S. Department of the Interior Office of Inspector General

Audit Report

IMPROVEMENTS MADE IN GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS

OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT



Picture courtesy of OSM

Report No. 01-I-415 September 2001

EXECUTIVE SUMMARY

Improvements Made in General Controls
Over Automated Information Systems,
Office of Surface Mining Reclamation and Enforcement
Report No. 01-I-415
September 2001

BACKGROUND

The Office of Surface Mining Reclamation and Enforcement (OSM) is dependent on automated information systems to support its mission and to provide reliable data for its annual financial statements. The Division of Information Systems Management is responsible for facilitating controls and efficient and effective use of information technologies and information resources to support the OSM mission.

OBJECTIVE

The objective of the audit was to determine whether the actions taken by the OSM satisfactorily implemented the 38 recommendations in our prior audit report titled "General and Application Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement," (No. 00-I-138) and whether any new recommendations were warranted.

RESULTS IN BRIEF

We concluded that the OSM had made substantial progress in correcting the weaknesses identified in our prior audit report and in improving general controls over the OSM's automated information systems. Based on actions taken previously and as a result of our current audit, we considered 37 of the 38 recommendations resolved and implemented.

RECOMMENDATIONS

We made four new recommendations to the OSM that should correct the weaknesses identified in our current report.

AUDITEE COMMENTS AND OFFICE OF INSPECTOR GENERAL COMMENTS The OSM concurred with the report's four recommendations and agreed to take the recommended corrective actions.



United States Department of the Interior

Office of Inspector General

National Information Systems Office 134 Union Boulevard, Suite 510 Lakewood, Colorado 80228

September 21, 2001

AUDIT REPORT

Memorandum

To: Director, Office of Surface Mining Reclamation and Enforcement

From:

Diann Sandy June Sandy Director, National Information Systems Office

Subject: Improvements in General Controls Over Automated Information Systems, Office of

Surface Mining Reclamation and Enforcement (No. 01-I-415)

We reviewed the actions taken by the Office of Surface Mining Reclamation and Enforcement (OSM) to determine whether the OSM satisfactorily implemented the 38 recommendations in our December 1999 audit report titled "General and Application Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement" (No 00-I-138) to improve general controls over the OSM's automated information systems. We also determined whether any new recommendations were warranted. In addition, we performed this audit to support the Office of Inspector General's opinion on the OSM's financial statements by evaluating the reliability of the general controls over automated systems that support the annual financial statements.

RESULTS OF AUDIT

The OSM **Improved** General **Controls Over** Its Automated Systems

We concluded that the OSM had made substantial progress in improving general controls over its automated information systems by implementing 37 of the 38 recommendations contained in our prior audit report. We found that before the start of our current audit, the OSM implemented 29 of the 38 recommendations from our prior audit. Based on our current audit, the OSM implemented an additional 8 recommendations. The one prior audit recommendation awaiting implementation pertains to contingency plans. Our current audit made four new recommendations concerning the completion of corrective actions and the improvement of security management and access controls.

The OSM recently improved controls in the following areas.

Risk Management

In our prior report we recommended that risk assessments be conducted (Recommendation A.2). The OSM prepared risk assessments of its five mission-critical information systems, and senior management approved these assessments.

Reviewing Users' Access to Systems

In our prior report we recommended that the OSM develop and implement procedures to periodically review users' levels of access to systems to ensure that the access levels are current and appropriate (Recommendation E.3). The OSM Division of Financial Management completed its review of access levels of all users of its systems, and the OSM has implemented procedures to ensure that periodic reviews of all users levels of access to all OSM systems would be performed.

Notifying System Administrators of Changes in Users' Employment Status

In our prior report we recommended that the OSM develop and implement procedures to promptly notify system administration personnel of users' employment terminations or reassignments of duties (Recommendation E.4). The OSM developed procedures for promptly notifying system administration personnel of system users' employment terminations or reassignments.

Separation of Duties

In our prior report we recommended that policies and procedures be implemented to ensure separation of duties between reviewing and controlling system logs and administering system access controls (Recommendations K.3 and M.1). In addition, we recommended that application programmers should not be responsible for moving changed software into the production environment and should not have access to update or change production data (Recommendation M.2). The OSM developed policies and procedures for maintaining, controlling, and reviewing system logs and ensured that personnel who were responsible for maintaining the logs did not review or control the logs or administer access to the systems. In addition, the OSM implemented procedures, which it believes alleviates the separation of duty risks, for moving changed software to the production environment. Further, in the OSM's next risk analysis, the OSM

will address the risk associated with the separation of duties in moving changed software into production and ensure that OSM management officials accept any residual risk.

Software Development and Change Management Controls

In our prior report we recommended that the OSM's policies and procedures for software development and change management be enforced (Recommendation N.1). The OSM developed policies to ensure that all application software changes are properly authorized, tested, and approved prior to being moved into production and that access to software programs is controlled. In addition, the OSM established an Independent Security Officers Review Team to perform periodic reviews of software development and change management to ensure that OSM policies are followed.

Further
Improvement in
System Security
Management and
Access Controls
Are Needed

We found that further improvements are needed in the following areas.

Finalize and Test System Contingency Plan

In our prior report we recommended that contingency plans intended for telecommunications links, facilities, and the data center be finalized and tested and that test results be used to update these plans. Additionally, we recommended that assurance should be provided that personnel are trained to implement the plans (Recommendation O.2). The OSM had not finalized the systems contingency plan and had not tested the continuity of operations plan for the OSM headquarters operations. The OSM officials said that the planning for service continuity was ongoing but the plan had not been completed, approved, and finalized. Until the headquarters contingency planning is completed and tested, the OSM remained vulnerable to loss of systems operations caused by a loss of computing capability due to an unexpected event.

Reevaluate Position Sensitivity Classifications

Although the OSM implemented personnel security policies and procedures, we found that position sensitivity classifications were not always based on the duties and risks of the positions. For example, system administrator positions that had full access and control over systems were not designated as critical public trust positions. Without adequate classification of positions warranting critical public trust and the commensurate security clearances, the risk was increased that the OSM systems could be compromised or impaired. The OSM needs to reevaluate its positions for

performing information systems duties to determine the inherent security risks and sensitivity of these positions and properly classify the positions of high risk.

New User Access

The OSM policy requires granting access to new users of systems to be documented and approved by system security managers or system owners. We found, however, that access was granted to the Applicant Violator System (AVS), which is a major application, based on verbal requests via telephone communication. Granting access to the AVS by verbal request does not ensure that the request is authentic and that responsible managers or supervisors have authorized the new user access request. Using this type of authorizing procedure subjects the AVS to the risk of unauthorized use and uncontrolled acts. The OSM needs to ensure that new user access to the AVS is granted in accordance with established OSM access control procedures.

Remote Access

The OSM had established remote access connectivity to some of its information systems via dialup to a modem pool; however, all available security practices to control unauthorized dialup access were not implemented. For example, we found that the telephone numbers for the remote-access modem pool were not periodically changed and that a call-back feature to specifically authorized remote-user telephone numbers was not implemented. Additionally, the OSM had not established other available security measures for remote-access users (via modem and the Internet from home computers) such as requiring specific virus protection on the remote computers. The OSM management needs to strengthen remote access controls and safeguards to protect the OSM systems from unauthorized intrusion, virus threats, and cyber attacks.

Recommendations

We recommend that the Director, OSM:

1. Fully implement our prior report Recommendations A.2, C.1, E.3, E.4, K.3, M.1, M.2, N.1, and O.2; or institute other alternative or compensating controls adequate to correct the weaknesses; or if certain weaknesses are an acceptable risk, document the risk acceptance in a formal (management approved) risk assessment.

- 2. Reevaluate the appropriateness of designated sensitive or high risk positions and the respective duties and obtain the necessary security clearances for personnel filling these sensitive or critical public trust positions.
- 3. Ensure that the OSM's established policies and procedures are followed when granting new users' access to the Applicant Violator System.
- 4. Establish remote-access control procedures and remote user-set parameters and strengthen the existing practices by providing added control features and required settings or document the acceptance of risk in a formal (management approved) risk assessment.

OSM Response and OIG Reply

Based on the May 30, 2001 (Appendix 2) and July 3, 2001 (Appendix 3) responses, we consider Recommendation 1 resolved but not implemented and have requested additional information for Recommendations 2, 3, and 4. The OSM agreed with the recommendations, but needs to provide target dates for implementation of actions planned and titles of officials responsible for implementation. The May 30, 2001 response to Recommendation 1 stated that the only remaining corrective actions regarding our prior report's recommendations would be to complete Recommendation O.2 during June and August 2001. Additionally, the OSM provided the latest draft version of the Continuity of Operations Plan (Management Plan, Test Plan, and Schedule) for its headquarters systems operations. As stated in the Results of Audit section, the OSM draft plan still needs to be finalized and tested.

Background

The mission of the OSM is to implement the provisions of the Surface Mining Control and Reclamation Act and to ensure that society and the environment are protected from the adverse effects of surface and subsurface coal mining operations. The OSM activities include issuing mining permits, inspecting mining operations, enforcing mining standards, ensuring the effectiveness of authorized state and tribal regulatory programs, and promoting reclamation of surface mine lands.

The OSM is dependent on automated information systems to support its mission and provide reliable data for its financial statements. The Division of Information Systems Management is responsible for facilitating the systems controls and efficient and effective use of information technologies to support the OSM mission. Various OSM organizations, including the Division of Information Systems Management, the Division of Financial Management, assistant directorates, and regional and field offices share responsibilities over the OSM systems. Nationwide, automated data processing support is provided through local area

network-based servers and microcomputer workstations, and the networks are interconnected by the OSM-wide area network.

Scope and Methodology

Our audit was conducted at the OSM's headquarters in Washington, D.C., and its data center in Denver, Colorado. Our audit was performed in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of the records and other auditing procedures that were considered necessary under the circumstances. Additionally we used the review methodologies contained in the U.S. General Accounting Office's "Federal Information System Controls Audit Manual." As part of our review we evaluated only the internal controls related to the general control environment over the OSM's automated information systems.

Section 5(a) of the Inspector General Act (5 U.S.C. app. 3) requires the Office of Inspector General to list this report in its semiannual report to the Congress. In addition, the Office of Inspector General provides audit reports to the Congress.

This report is intended for the information of management of the Department of the Interior, the Office of Management and Budget, and the Congress. However, this report is a matter of public record, and its distribution is not limited.

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR THE DECEMBER 1999 AUDIT REPORT "GENERAL AND APPLICATION CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT" (No. 00-I-138)

Recommendations	Status of Recommendations and Corrective Actions
A.1. Determine the risks associated with each of the	Implemented.
systems and, based on the results of the risk assessments,	
establish appropriate security policies and procedures.	
A.2. Ensure that risk assessments are conducted in	Implemented.
accordance with Federal guidelines which recommend that	
risk assessments support the acceptance of risk and the	
selection of appropriate controls. Specifically, the risk	
assessments should address significant risks affecting	
sensitive systems and major applications, appropriately	
identify controls implemented to mitigate those risks, and	
formalize the acceptance of residual risk.	
A.3. Formally assign and communicate responsibility to	Implemented.
those individuals required to participate in assessing risks.	
B.1. Provide resources to ensure that automated	Implemented.
information systems security plans are developed for the	
OSM's general support systems and major applications in	
accordance with the Computer Security Act; Office of	
Management and Budget Circular A-130, Appendix III; and	
the National Institute of Standards and Technology's	
Special Publication 800-18.	
B.2. Ensure that the automated information systems	Implemented.
security function is elevated organizationally to report	
directly to the OSM's Chief Information officer and	
formally provide the position with the authority to	
implement and enforce a computer security program	
throughout the OSM.	
B.3. Report the lack of security plans for the OSM's	Implemented.
sensitive systems as a material weakness in the OSM's	
annual assurance statement on management controls for	
fiscal year 1999.	
C.1. Ensure that personnel security policies and procedures	Implemented.
are developed, implemented, and enforced, including those	
for obtaining appropriate security clearances for personnel	
filling sensitive or critical public trust positions.	
C.2. Ensure that all automated data processing contractor	Implemented.
employees have proper background clearances.	

Recommendations	Status of Recommendations and Corrective Actions
C.3. Ensure that periodic reinvestigations are completed every 5 years on personnel who are in public trust high risk positions.	Implemented.
D.1. Develop and implement policies to classify the OSM's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A-130, Appendix III.	Implemented.
E.1. Institute a policy of "least privilege" access levels to ensure that access to resources and data is limited to those users who require such access.	Implemented.
E.2. Develop and implement policies and procedures for approving access to the automated information systems that include the formal assignment of responsibility for approving systems access.	Implemented.
E.3. Develop and implement procedures to ensure that user access levels are periodically reviewed to ensure that the current access provided is appropriate.	Implemented.
E.4. Develop and implement procedures to ensure that system administration personnel are promptly notified of changes in employee assignments or employment terminations.	Implemented.
E.5. Implement controls to ensure that system owners approve all access to their applications in accordance with the OSM's policy.	Implemented.
F.1. Develop and implement policies and procedures establishing the maximum number of log-in attempts allowed for the OSM's automated information systems in compliance with Department of the Interior regulations.	Implemented.
F.2. Ensure that the systems log-in warning message is the first screen displayed upon initial access and prior to the user being authenticated as a valid system user.	Implemented.
G.1. Develop and implement password policies and procedures. In addition, controls to ensure compliance with these policies and procedures should be implemented.	Implemented.
G.2. Implement a policy requiring system administration personnel to log on to the automated information systems under specific user IDs.	Implemented.
G.3. Evaluate current capabilities and implement procedures to address encryption or other security methods to help prevent powerful system passwords and accounts from being compromised when traveling across a network, such as the wide area network and the Internet.	Implemented.

Recommendations	Status of Recommendations and Corrective Actions	
H.1. Develop policies and procedures to ensure that controls are in place to protect the Novell network operating system and other system software from unauthorized modification or manipulation.	Implemented.	
I.1. Identify and implement the technical controls necessary to ensure that only authorized users have access to the Novell file servers. The controls should include using the "SECURE CONSOLE" command in the autoexec.ncf file, encrypting the "RCONSOLE" password, and using the "LOCK CONSOLE" command.	Implemented.	
J.1. Install a firewall system for the Division of Financial Management's local area network.	Implemented.	
K.1. Evaluate acquiring systems verification and auditing software.	Implemented.	
K.2. Implement the systems options available in each of the operating systems to record activities affecting the systems.	Implemented.	
K.3. Implement policies and procedures to ensure that systems logs are used and are maintained for an appropriate amount of time to provide an adequate audit trail of systems activities and are controlled by personnel independent of the systems access control administration function.	Implemented.	
K.4. Develop and implement procedures to ensure that periodic reviews of systems logs for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to the OSM management.	Implemented.	
L.1. Establish policy and procedures for ensuring that available software updates and service packs are reviewed to identify those that should be implemented to address an applicable systems vulnerability.	Implemented.	
L.2. Implement procedures to ensure that those updates which are determined to be needed are implemented in a timely manner.	Implemented.	
M.1. Implement procedures to ensure that personnel who perform access control administration are not the same individuals who review and control systems security logs and systems audit trails.	Implemented.	
M.2. Implement controls to ensure that application programmers are not responsible for moving changed software into the production environment and do not have access to update/change production data.	Implemented.	

Recommendations	Status of Recommendations
Recommendations	and Corrective Actions
N.1. Enforce OSM's written policies and procedures to	Implemented.
ensure that all application programs and modifications are	
properly authorized, tested, and approved and that access to	
and distribution of programs is controlled.	
N.2. Establish the process of correcting applications	Implemented.
deficiencies as a high priority to reduce manual processes.	
N.3. Review change requests timely to ensure that user	Implemented.
requirements are supported in the applications.	
O.1. Ensure that a contingency plan is developed for critical	Implemented.
telecommunications links.	
O.2. Ensure that contingency plans for telecommunications	Partially implemented. The
links, facilities, and the data center are finalized and tested	OSM had not completed and
and that test results are used to update these plans.	finalized its contingency plans
Additionally, assurance should be provided that personnel	or fully tested the plan for its
are trained to implement the plans.	headquarters operations.
O.3. Provide for a secure off-site storage facility that is at	Implemented.
least 1 mile from the computer facility.	
P.1. Develop and implement a formal incident response	Implemented.
plan and team.	



United States Department of the Interior

OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT Washington, D.C. 20240

MAY 23 2001

MEMORANDUM

To:

Roger LaRouche

Assistant Inspector General for Audits

Through:

Piet deWitt, Acting Assistant Secretary (AV 3 0 200

Lands and Mineral Managemen

From:

Glenda Owens, Acting Director

Office of Surface Mining Reclamation and Enforcement

Subject:

Draft Audit Report on Implementation of Recommendations for Improving the General Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement (Assignment Number A-IN-OSM-001-00-M)

This response is to the subject Draft Audit Report on Implementation of Recommendations for Improving the General Controls over Automated Information Systems at the Office of Surface Mining (OSM).

The audit was conducted to determine whether OSM had satisfactorily implemented the 38 recommendations from the December 1999 audit report titled "General and Application Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement" (No. 00-I-138) and to determine whether any new recommendations were warranted. In addition, this audit supported the Office of Inspector General's opinion on the OSM's financial statements by evaluating the reliability of the general controls over automated systems that support the annual financial statements.

The Draft Audit Report concluded that the OSM had made substantial progress in correcting the weaknesses identified in the prior Audit Report and in improving the general controls over its automated information systems by implementing 29 of the 38 recommendations. Of the remaining nine recommendations, the OSM had taken actions to partially implement six, and had not taken any action to implement three of the recommendations. This response will address each of the six partially implemented recommendations, and the three recommendations which OSM has not taken any action on implementing.

If you have questions or require additional information regarding this response, please have your staff contact Donald Griffith on 202-208-2916, or by e-mail: dgriffit@osmre.gov.

Attachment

Note: ALL ATTACHMENTS NOT INCLUDED BY OFFICE OF THE INSPECTOR GENERAL.

OFFICE OF SURFACE MINING RESPONSE TO IG AUDIT RECOMMENDATIONS MAY 29, 2001

OSM reviewed the Draft Audit Report Number A-IN-OSM-001-00-M, and concurs with the IG conclusion that OSM has made substantial progress in correcting the weaknesses identified in the prior IG Audit Report number 00-I-138, and in improving the general controls over its automated information systems by implementing 29 of the 38 recommendations identified in the prior audit report. In addition, OSM also agrees with the IG conclusion, that of the remaining nine recommendations, the OSM has taken actions to partially implement six recommendations and has not taken the necessary actions to implement three recommendations.

The following response address both the six partially implemented recommendations and the three recommendations which OSM has not taken the necessary actions to implement:

RECOMMENDATIONS:

A.2. Ensure that risk assessments are conducted in accordance with the Federal guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the risk assessments should address significant risks affecting sensitive systems and major applications, appropriately identified controls implemented to mitigate those risks, and formalize the acceptance of residual risk.

Response: OSM concurs with the IG on this item and offers the following response:

OSM completed a risk assessment for each of its 5 mission critical systems and has established security policies and procedures. However, the assessments had not been approved my management at the time of the IG audit review. The risk assessments have now been approved by management, and copies of the approved risk assessments are at attachment I.

C.1. Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel filling sensitive or critical public trust positions.

Response: OSM concurs with the IG on this item and offers the following response:

OSM has developed a Security Directive (copy at attachment II), which contains personnel security policies and procedures for obtaining appropriate security clearances for personnel filling sensitive and critical trust positions. In addition, Chapter VI of the Security Directive provides guidance on how to designate position sensitivity for all

OSM positions, and the level of background investigation which should be completed on each type of position.

The office of Personnel has identified personnel in Sensitive Computer areas and their position risk designation to ensure proper clearance and background investigations are completed. However, OSM agrees with the IG that position sensitivity classifications of critical public trust positions were not always appropriately based on the duties and risks of the position, and these computer positions were re-evaluated and updated with the responsible management official.

E.3. Develop and implement procedures to ensure that user access levels are periodically reviewed to ensure that the current access provided is appropriate.

Response: OSM Concurs with the IG on this item and offers the following response:

OSM has included procedures in Chapter XII, Section D of the Security Directive that user access levels are periodically reviewed to ensure that access levels provided are appropriate. OSM requires that all system administrators complete a total review of all User access privileges periodically. OSM agrees with the IG finding that reviews of users' access levels were not performed on all information systems. However, to ensure that these reviews are conducted, OSM has established an Independent Security Oversight Review Team (ISORT) to audit our information systems agency wide and ensure that procedures outlined in the Security Directive, which includes reviewing access levels are being followed.

DFM's Site Information Security Officer (SISSO), issued an e-mail to all System Administrators and System Owners that a complete review of all users' access levels for all systems and platforms must be completed by May 15, 2001. This review was completed on May 15, 2001, and a copy of the e-mail is at attachment III. DFM will continue to perform these reviews periodically.

E.4. Develop and implement procedures to ensure that system administration personnel are promptly notified of changes in employee assignments or employment terminations.

Response: OSM concurs with the IG on this item and offers the following response:

The OSM Employee Exit Clearance Form has been updated to include a section for the supervisor of the employee being reassigned or terminated to sign. The signature will remind the supervisor of this responsibility to immediately notify the key managers and systems owners that an employee has changed his status. The OSM e-mail system has been updated to assist the supervisor with this responsibility. The supervisor only needs to send an e-mail to "Clearance" and the e-mail will automatically be routed to key managers and all system owners to ensure that the employee's access is removed from all information systems. To ensure that these procedures are fully implemented, the Office

of Personnel e-mails a monthly list of separated employees to key OSM system owners, management and staff for their review.

K.3. Implement policies and procedures to ensure that systems logs are used and are maintained for an appropriate amount of time to provide an adequate audit trail of systems activities and are controlled by personnel independent of the systems access control administration functions.

Response: OSM concurs with the IG on this item and offers the following response:

OSM has developed policies and procedures to ensure that systems logs are used and maintained. Both the SUN and HP computers systems at DFM maintain and retains system logs for a period of six months. The audit functions on both the NT and Novell servers in Washington are enabled. However, OSM agrees with the IG's conclusion that systems logs are not controlled by Personnel independent of the systems access administration function.

To fully implement this recommendation in Washington, D.C., OSM has assigned the NT administrator to oversee the system logs for the Novell servers and assigned the Novell administrator to oversee the systems logs for the NT servers. In Denver, DFM has implemented a policy requiring that both the primary and backup system administrator review the system logs.

M.1. Implement procedures to ensure that personnel who perform access control administration are not the same individuals who review and control systems security logs and systems audit trails.

Response: OSM concurs with the IG on this item and offers the following response:

DFM has procedures in place to ensure that personnel who perform access control administration are not the only individuals who review and control system security logs and system audit trails. DFM has implemented procedures requiring that both the primary and backup system administrator review the system logs, and that the system owners review system audit trails.

M.2. Implement controls to ensure that application programmers are not responsible for moving changed software into the production environment and do not have access to update/change production data.

Response: OSM concurs with the IG on this item and offers the following response:

Due to staffing levels, DFM is unable to provide for complete separation of duties as indicated by this finding. DFM has implemented procedures for the movement of changed software into our production environment that we feel alleviates the risks associated with this finding. In the next update of our risk analysis documents, we will

specifically address each of these risks, the controls in place, and the request that management approve the procedure we have established as appropriate. The Financial and Administrative Systems Team Leader has conveyed to all team leaders, system accountants, programmers, and system administrators that these procedures are to be strictly adhered to, with no exceptions. DFM will adhere to this process and obtain all signatures before software is moved into the production environment.

N.1. Enforce OSM's written policies and procedures to ensure that all application programs and modifications are properly authorized, tested, and approved and that access to and distribution of programs is controlled.

Response: OSM concurs with the IG on this item and offers the following response:

OSM has developed policies and procedures to ensure that all application program modifications are properly authorized, tested, approved and that access to and distribution of programs are controlled. This policy is in Chapter XII, Section H and Chapter IV, Section D of the Security Directive. To ensure that these policies are adequately enforced, OSM has established and implemented an Independent Security Officers Review Team to audit OSM's information systems agency wide and ensure that policies are being followed.

OSM agrees with the IG Report that we were not always following our own written procedures, however, the IG did agree in the exit interview that the process used at DFM for implementing system and software changes was adequate. It has been conveyed to the appropriate staff at DFM that these procedures will be strictly adhered to, with no exceptions, and all signatures must be obtained before any software is moved into a production environment.

O.2. Ensure that contingency plans for telecommunications links, facilities, and the data center are finalized and tested and that test results are used to update these plans. Additionally, assurance should be provided that personnel are trained to implement the plans.

Response: OSM concurs with the IG on this item and offers the following response:

OSM has and tested its Washington, D.C., Headquarters contingency plans, and made modifications to the contingency plans, where appropriate. A copy of the test plans and results are in attachment IV.

OFFICE OF SURFACE MINING RESPONSE TO IG AUDIT RECOMMENDATIONS JULY 3, 2001

OSM reviewed the Draft Audit Report Number A-IN-OSM-001-00-M, and has concurred with the IG conclusions that OSM has made substantial progress in correcting the prior identified weaknesses. In our last response to this Draft Audit report we neglected to comment on items listed under **Recommendations** made to the Director, OSM. Our comments are as follows:

2. Reevaluate the appropriateness of designated sensitive or high risk positions and the respective duties and obtain the necessary security clearances for personnel filling these sensitive or critical public trust positions.

Response: OSM concurs with the IG on this item and offers the following response:

OSM will reevaluate the appropriateness of designated sensitive or high risk positions and respective duties and obtain the necessary security clearances. The security clearance of the position with be commensurate with actual duties and access to information and systems.

3. Ensure that the OSM's established policies and procedures are followed when granting new users' access to the Applicant Violator System.

Response: OSM concurs with the IG on this item and offers the following response:

OSM will ensure that established policies and procedures are followed when granting new users' access to the Applicant Violator System. All new user access from within OSM or from the States and Tribes will have the appropriate documentation prior to the issuance of access.

4. Establish remote-access control procedures and remote user-set parameters and strengthen the existing practices by providing added control features and required settings or document the acceptable risk in a formal (management approved) risk assessment.

Response: OSM concurs with the IG on this item and offers the following response:

OSM is currently reviewing our remote-access procedures and will implement procedures to increase security. Remote-access guidelines for granting user access will be reviewed to keep access to an as needed basis. Current accounts have been reviewed and inactive accounts deleted.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/ Recommendation Reference	Status	Actions Required
1	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
2, 3, and 4	Management concurs; additional information requested.	Provide the Office of Inspector General with target dates for actions planned and titles of officials responsible for implementation.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL

Internet Complaint Form Address http://www.oig.doi.gov/hotline form.html

Within the Continental United States

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Washington, D.C. 20240-0001 Our 24-hour Telephone HOTLINE 1-800-424-5081 or (202) 208-5300

TDD for hearing impaired (202) 208-2420

Outside the Continental United States

Caribbean Region

U.S. Department of the Interior

(703) 235-9221

Office of Inspector General Eastern Division – Investigations 4040 Fairfax Drive Suite 303 Arlington, Virginia 22203

Pacific Region

U.S. Department of the Interior Office of Inspector General Guam Field Pacific Office 415 Chalan San Antonio Baltej Pavilion, Suite 306 Agana, Guam 96911 (671) 647-6060



U.S. Department of the Interior Office of Inspector General

AUDIT REPORT

GENERAL AND APPLICATION CONTROLS
OVER AUTOMATED INFORMATION SYSTEMS,
OFFICE OF SURFACE MINING
RECLAMATION AND ENFORCEMENT

REPORT NO. 00-I-138 DECEMBER 1999



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL Washington, D.C. 20240

DEC 211999

AUDIT REPORT

Memorandum

To: Director, Office of Surface Mining Reclamation and Enforcement

From: Robert J. Williams Wobert & Williams

Assistant Inspector General for Audits

Subject: Audit Report on General and Application Controls Over Automated

Information Systems, Office of Surface Mining Reclamation and Enforcement

(**No.** 00-I-138)

INTRODUCTION

This report presents the results of our audit of the Office of Surface Mining Reclamation and Enforcement's general and application controls over its automated information systems. The objective of this audit was to determine whether Surface Mining had effective general and application controls over its automated information systems and whether the automated information systems were operating in compliance with the Federal Financial Management Improvement Act. We performed this audit to support the Office of Inspector General's opinion on the financial statements of Surface Mining by evaluating the reliability of the general and application controls over computer-generated data that support Surface Mining's annual financial statements.

BACKGROUND

The Office of Surface Mining Reclamation and Enforcement was created with the enactment of the Surface Mining Control and Reclamation Act of 1977 (Public Law 95-87). The purpose of Surface Mining is to implement the provisions of the Surface Mining Control and Reclamation Act and to ensure that society and the environment are protected from the adverse effects of surface and subsurface coal mining operations. Surface Mining meets this mission through programs authorized by Title IV (Abandoned Mine Reclamation) and Title V (Control of the Surface Effects of Coal Mining) of the Surface Mining Control and Reclamation Act. Surface Mining's activities include issuing mine permits, inspecting mine operations, enforcing mine standards, ensuring the effectiveness ofauthorized state and tribal regulatory programs, and promoting reclamation of surface mine lands.

Surface Mining has its headquarters in Washington, D.C., and has decentralized its regulatory and enforcement mission through the Appalachian Regional Coordinating Center, in Pittsburgh, Pennsylvania; the Mid-Continent Regional Coordinating Center, in Alton, Illinois; and the Western Regional Coordinating Center, in Denver, Colorado. Additionally, Surface Mining maintains a close working relationship with governments of the coal-producing states, environmental protection groups, and mission support contractors.

Surface Mining is dependent on automated information systems to support its mission and financial statements. The Division of Information Systems Management is responsible for facilitating the efficient and effective use of information and information technologies in support of information resources management and Surface Mining's mission. The information resources management responsibilities are shared by various Surface Mining organizations, including the Division of Information Systems Management, the Division of Financial Management, assistant directorates, and regional and field offices. Nationwide, automated data processing support is provided through local area network-based microcomputer workstations, including Windows NT, Silicon Graphics, and Sun Solar-is UNIX. The local area networks are interconnected by Surface Mining's wide area network.

The data center responsible for inputting, recording, classifying, and reporting on Surface Mining's financial business is located at the Division of Financial Management in Denver. The Division operates and maintains two minicomputer platforms, a Hewlett Packard and a Sun Solaris, to support Surface Mining's financial management functions. The Hewlett Packard computer hosts Surface Mining's primary financial management system, the Advanced Budget/Accounting Control and Information System (ABACIS). In addition, the Hewlett Packard computer hosts other financial applications that affect the generation of financial statement information as follows:

- The Grants Information Fund Tracking System (GIFTS)
- The Civil Penalty Accounting Control System (CPACS)
- The Audit Fee Billing and Collection System (AFBACS)
- The Synergistic Acquisition Tracking and Information Network (SATIN)

The Sun Solaris computer hosts the Fee Billing and Collection System (FEEBACS) application, which generates records for posting to ABACIS and affects the generation of financial statement information. In addition, FEEBACS supports Surface Mining's mission critical Applicant Violator System (AVS), which is an independent, stand-alone system that does not generate data for or impact Surface Mining's financial records and statements. Also, the Division operates a Windows NT computer network that distributes personnel data to Surface Mining's human resource and budget personnel and provides financial management data to Surface Mining's users.

Systems security policies for Surface Mining are established by its Information Technology Security Officer. System security administration for the minicomputers, local area networks, and the wide area network is the responsibility of the information technology security officers at Surface Mining offices and facilities.

SCOPE OF AUDIT

We reviewed Surface Mining's general controls (the policies and procedures for ensuring that information systems operate properly) that were in place for its automated information systems. We did not review the application controls (the controls over input, processing, and output of data) because of the weaknesses we found in the general controls. The effectiveness of the general controls determines the effectiveness of the application controls. When the general controls are not effective, application controls can be made ineffective because the application controls can be bypassed or modified.

We reviewed the general controls in six major areas: security program development, logical and physical access, change management, separation of duties, system software, and service continuity. To accomplish our objective, we interviewed Surface Mining and contractor personnel, reviewed systems documentation, observed and became familiar with data center operations and network components, analyzed systems security, and evaluated service continuity procedures and testing. In addition, we reviewed the software maintenance procedures. During the audit, we used several software tools to identify vulnerabilities in Surface Mining's automated information systems and networks. These tools were used to perform a variety of functions, such as monitoring and analyzing user and system activity, auditing system configurations and vulnerabilities, accessing the integrity ofcritical systems and data files, and operating system audit-trail management. Because our review was limited to evaluating the adequacy of general controls over automated information systems, we did not evaluate the effectiveness of manual control procedures that may have operated as compensating controls for the automated information systems' general controls.

Our audit, which was conducted during January through April 1999 at Surface Mining's headquarters and the data center in Denver, Colorado, was made in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we evaluated the internal controls that could adversely affect Surface Mining's automated information systems. The control weaknesses that we found are summarized in the Results of Audit section and detailed in Appendix 1 of this report. Based on our determination of the inadequacy of the general controls taken as a whole, we believe that the weaknesses in Surface Mining's general controls over its automated information systems should be reported as a "reportable condition" in Surface Mining's annual financial statements for fiscal year 1999. In addition, Surface Mining did not have security plans for its 13 sensitive systems. We believe that Surface Mining should report the lack of security plans for the systems as a material weakness in its annual assurance statements on management controls for fiscal year 1999. Because of inherent limitations in any system of internal controls, losses, noncompliance, or misstatements may occur and not be detected. We also caution that projecting our evaluations to future periods is subject to the risk that controls or the degree of compliance with the controls may diminish.

PRIOR AUDIT COVERAGE

During the past 5 years, neither the General Accounting Office nor the Office of Inspector General has issued any reports related to the Office of Surface Mining Reclamation and Enforcement's general controls over its automated information systems.

RESULTS OF AUDIT

We concluded that the Office of Surface Mining Reclamation and Enforcement's general controls over its automated information systems were not effective. Specifically, Surface Mining did not have an adequate security program; did not have controls over access to automated information systems resources, systems software, separation of duties, and software development and change management; and did not have assurance of continued operations in the event of a disaster or system failure. Office of Management and Budget Circular A- 130, "Management of Federal Information Resources," and National Institute of Standards and Technology publications require Federal agencies to establish and implement computer security and management and internal controls to improve the protection of information in the computer systems of executive branch agencies. Additionally, the Congress enacted laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls over sensitive information is adequate. The Computer Security Act defines "sensitive" data as "any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act." Further, the Department of the Interior and Surface Mining have issued policies and procedures to implement general controls to protect sensitive data in automated information systems. However, the general controls were not adequate because Surface Mining management had not (1) established necessarypolicies and procedures for the controls, (2) assigned responsibilities for ensuring that policies and procedures were developed and followed, and (3) held officials accountable for noncompliance with the established controls. The lack of adequate controls increased the risk of unauthorized access and modifications to and the disclosure of Surface Mining data, theft or destruction of Surface Mining software and sensitive information, and loss of critical Surface Mining systems and functions in the event of a disaster or system failure.

Overall, we identified 16 weaknesses and made 38 recommendations for improving the general controls over Surface Mining's automated information systems. A summary of the weaknesses noted in the six major areas reviewed is provided in the paragraphs that follow, and specific details of the weaknesses and our respective recommendations to correct these weaknesses are in Appendix 1.

Security Program

We found that Surface Mining did not have an automated information systems security program which identified and addressed all risks affecting sensitive and financial data, did not have security plans for its 12 sensitive automated information systems, and did not have adequate security-related personnel policies and procedures for Surface Mining employees and contractors. As a result, there was an increased risk that sensitive data may be impaired or compromised by individuals and that data may be inadvertently disclosed, destroyed, or erroneously modified. We made nine recommendations to address these weaknesses.

Access Controls

We found that Surface Mining did not have adequate controls over access to its automated information systems. Specifically, Surface Mining did not classify its automated information systems resources to determine the level of security that should be provided, control the levels of access granted to systems users, limit the number of log-in attempts allowed for access to computer resources as required by Department of the Interior standards, control passwords and password settings, control public user access to the Novell network and file servers, and protect its local area networks. As a result, there was an increased risk that sensitive data maintained on the automated information systems were vulnerable to unauthorized access, manipulation, and disclosure. We made 14 recommendations to address these weaknesses.

System Software Controls

We found that the controls over system software did not detect and determine inappropriate use and address vulnerabilities in the operating systems. Specifically, available computer systems audit tools to ensure integrity over systems processing and data were not used, some systems audit trails were not implemented and when implemented were not reviewed, and vendor updates to operating systems software were not implemented. As a result, there was an increased risk that inappropriate systems settings and processing would not be identified and recorded. Also, without periodic reviews of the systems' audit trails, there was an increased risk that processing problems or unauthorized activities may not be detected or detected in a timely manner. Additionally, there was an increased risk that operating systems' vulnerabilities addressed by the vendor would not be corrected. We made six recommendations to address these weaknesses.

Separation of Duties

We found that Surface Mining management did not separate the duties of system security administrators from reviewers and did not separate the duties of the application programmers from systems users. As a result, there was an increased risk that inappropriate actions by security administrators would not be detected or detected timely and that accidental or intentional actions by programmers could threaten the integrity of Surface Mining's data and disrupt systems processing. We made two recommendations to address these weaknesses.

Software Development and Change Management

We found that Surface Mining did not ensure that changes to applications software were authorized, approved, and tested before being moved into production. As a result, there was an increased risk that critical sensitive applications software changes were not made and that applications would not perform as intended. We made three recommendations to address these weaknesses.

Service Continuity

We found that Surface Mining did not develop a continuity of operations plan for its telecommunications links, did not finalize plans for its facilities and data center, and did not have an incident response plan or team. As a result, there was an increased risk that critical systems or data may not be recovered in the event of a disaster or system failure. We made four recommendations to address these weaknesses.

Other Matters

During our audit, we also found that the environmental controls at Surface Mining's Information Systems Management computer operations room were not adequate to safeguard the computer resources. For example, the air conditioning system was not maintaining an appropriate room temperature; the carpeting was dirty and worn, which produces dust and debris; and the overall condition of the room was unkempt. The National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" states that computer resources, such as hardware, software, and magnetic media, require environmental protection to ensure that the computer resources are safeguarded from excessive temperatures, dust, and debris.

Office of Surface Mining Reclamation and Enforcement Response and Office of Inspector General Reply

In the September 17, 1999, response (Appendix 3) to the draft report from the Director, Office of Surface Mining Reclamation and Enforcement, Surface Mining concurred with the 38 recommendations. Based on the response, we consider Recommendations K.2, M. 1, M.2, N.2, O.2, O.3, and P. 1 resolved and implemented and Recommendation K. 1 resolved but not implemented. Accordingly, Recommendation K.1 will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (see Appendix 4). Regarding Recommendation B.3, we agree that the actions taken by Surface Mining to develop security plans for its mission critical systems are sufficient, although the plans are not complete; therefore, Surface Mining does not need to report this as a material weakness in the annual assurance statement on management controls for fiscal year 1999. Thus, we consider this recommendation resolved. Also based on the response, we request the dates and titles of the individuals responsible for implementing the remaining 30 recommendations.

Surface Mining has completed or has begun actions needed to implement the 38 recommendations. Specifically, the draft publication "Information Systems Security Program Directive" addresses many of our recommendations for developing policies and procedures to ensure that Surface Mining's automated systems are adequately safeguarded. Although Surface Mining has initiated actions to correct the general control weaknesses identified in this report, many of these actions were not completed by the end of fiscal year 1999. Therefore, we believe that the weaknesses in Surface Mining's general controls over its automated information systems should be reported as a "reportable condition" in Surface Mining's annual financial statements for fiscal year 1999.

Surface Mining's specific comments to some of the recommendations are in the paragraphs that follow.

Recommendation A.1. Surface Mining said that it had completed a risk assessment for each of its 16 mission critical systems and that these risk assessments were included in its response. However, the response did not include risk assessments for the Administrative Records Management System (ARMS); the Technical Information Processing System (TIPS); and the Work Assignment Tracking System/Mine Information, Project Planning System (WATS/MIPPS). Therefore, Surface Mining should complete risk assessments for these systems and provide target dates and titles of officials responsible for implementation.

Recommendation B.I. Surface Mining requested that we delete the Payroll/Personnel Data Entry (PAY/PERS) from our list of 13 sensitive systems because the System "is no longer used" by Surface Mining. Also, Surface Mining identified four additional systems requiring security plans. We have revised Appendix 2 to reflect these changes.

Recommendation B.2. Surface Mining said that it concurred with the recommendation; however, Surface Mining also said that it will elevate the information systems security function to report to the Deputy Chief Information Officer rather than to the Chief Information Officer (as we had recommended). We believe that this action meets the intent of the recommendation, but a target date and title of the official responsible for implementation should be provided.

Recommendation F.5. Surface Mining stated that the systems' log-in warning message cannot be the first screen displayed because of computer "hardware and operating system architecture." However, Surface Mining stated that the log-in warning message will be placed as close to the first screen as the hardware and operating system will allow. We believe that this action meets the intent of the recommendation, but a target date and title of the official responsible for implementation should be provided.

Recommendation K.3. Surface Mining said that the minicomputer platforms used by the Division of Financial Management maintain system logs and that the logs are retained for 6 months. Surface Mining also said that the audit function on the Windows NT and the Novell servers has been "enabled." However, Surface Mining needs to implement policies and procedures to ensure that the system logs are used and that the logs are controlled by

request that Surface Mining provide an action plan that includes a target date and title of the official responsible for implementing the policies and procedures.

In accordance with the Departmental Manual (360 DM 5.3), we are requesting a written response to this report by January 24, 2000. The response should provide the information requested in Appendix 4.

Section 5(a) of the Inspector General Act (Public Law 95-452, as amended) requires the Office of Inspector General to list this report in its semiannual report to the Congress. In addition, the Office of Inspector General provides copies of audit reports to the Congress.

We appreciate the assistance of Surface Mining personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

SECURITY PROGRAM

Control Objective: The control objective for the security program is to establish the framework for continually managing risk, developing system security policy, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

A. Risk Assessments

Condition: The Office of Surface Mining Reclamation and Enforcement did not implement a risk management process. Specifically, we found that:

- Risk assessments had not been made of Surface Mining's computer systems, applications, and computer resources.
- No overall determination had been made of the effectiveness of the technical controls implemented.
- No acceptance of the residual risk of not implementing a risk management process had occurred.

Criteria:

Office of Management and Budget Circular A- 130, Appendix III, "Security of Federal Automated Information Resources," states that adequate security "includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls." Circular A-130 further states that, although formal risk analyses need not be performed, adequate security should be determined based on risk management. In implementing risk management, major factors such as "the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards" should be considered. Also, the National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" provides guidance on computer security risk management. The "NIST Handbook" specifically addresses the selection of safeguards to reduce risk and to accept any residual risk.

Cause:

Surface Mining had not developed policies and procedures to establish a risk-based approach to assessing the risks to its automated information systems and taking actions to manage these risks. In addition, no one was formally assigned responsibility for conducting risk assessments; thus, risks to the automated information systems had not been identified and managed.

Effect:

Without identifying all significant threats and vulnerabilities to the automated information systems, computer resources, and facilities, Surface Mining's management was unable to determine the most effective measures needed to protect against threats or reduce the vulnerabilities. Therefore, there was a risk that critical Surface Mining resources would not be adequately protected and that expensive controls would be implemented for resources which did not require significant protection.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Determine the risks associated with each of the systems and, based on the results of the risk assessments, establish appropriate security policies and procedures.
- 2. Ensure that risk assessments are conducted in accordance with Federal guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the risk assessments should address significant risks affecting sensitive systems and major applications, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of residual risk.
- **3.** Formally assign and communicate responsibility to those individuals required to participate in assessing risks.

B. System Security Plans

Condition: Security plans for Surface Mining's 13 sensitive automated information systems (the systems are listed in Appendix 2) as reported to the Department of the Interior in Surface Mining's "Automated Information Systems Security Plan," dated February 1998, had not been developed. Also, Surface Mining had not reported the lack of security plans for the systems as a material weakness in its annual assurance statement on management controls for fiscal year 1999, as required by Office of Management and Budget Circular A-130, Appendix III.

Criteria:

The Computer Security Act of 1987 requires the development of a security plan for each Federal computer system that contains sensitive information. A computer security plan is designed to assist agencies in addressing the protection of general support systems' and major applications that contain sensitive information to help ensure the systems' integrity, availability, and confidentiality. In addition, Office of Management and Budget Circular A- 130, Appendix III, states that agencies without adequate security plans should consider classifying the lack of security plans as a material weakness in the agency's annual Federal Managers' Financial Integrity Act report to the Congress. Also, the National Institute of Standards and Technology's Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," states that "[a]!! Federal systems have some level of sensitivity and require protection as part of good management practice" and that the method of protection must be documented in a system security plan.

Cause:

Surface Mining management, rather than developing security plans for its 13 sensitive systems, said that it believed the Management Control Reviews and Alternative Management Control Reviews were sufficient to meet security plan requirements. In addition, because Surface Mining's information technology security function was within the Division of Information Systems Management's Automated Data Processing Support Team, the function did not have adequate independence and authority to implement and enforce an overall Surface Mining computer security program that would ensure that security plans were developed for Surface Mining's general support systems and major applications. We believe that, at a minimum, the position of Information Technology Security Officer should be elevated to report directly to Surface Mining's Chief Information Officer. Further, while Surface Mining had

^{&#}x27;General support systems are an interconnected set of information resources under the same direct management control which shares common functionality.

information technology security officers at other locations, most of their time was spent in performing other duties.

Effect:

Without automated information systems security plans, Surface Mining's management did not have adequate assurance that the data in its sensitive systems were adequately protected. In addition, without security plans for the 13 sensitive systems, Surface Mining had a material weakness that should be reported in its annual assurance statement on management controls for fiscal year 1999.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Provide resources to ensure that automated information systems security plans are developed for its general support systems and major applications in accordance with the Computer Security Act; Office of Management and Budget Circular A-130, Appendix III; and the National Institute of Standards and Technology's Special Publication 800-1 8.
- **2.** Ensure that the automated information systems security function is elevated organizationally to report directly to Surface Mining's Chief Information Officer and formally provide the position with the authority to implement and enforce a computer security program throughout Surface Mining.
- 3. Report the lack of security plans for Surface Mining's sensitive systems as a material weakness in Surface Mining's annual assurance statement on management controls for fiscal year 1999.

C. Security-Related Personnel Policies and Procedures

Condition: Surface Mining's security-related personnel policies and procedures did not ensure systems integrity. Specifically, we found that:

- Surface Mining personnel in public trust positions, such as computer security officers, system and application programmers, and sensitive automated information system owners and managers, did not have documented background investigations for security clearances or did not have adequate position sensitivity levels commensurate with their positions. Also, Surface Mining personnel did not have documentation to support that required periodic followup background checks had been performed.
- Critical automated data processing contractor personnel, such as system administrators and software management personnel, at the Division of Information Systems Management did not have documented background checks and security clearances.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish and manage personnel security policies, standards, and procedures that include requirements for screening individuals who (1) participate in the design, development, operation, or maintenance of sensitive applications or (2) have access to sensitive data. Also, the Code of Federal Regulations (5 CFR 73 1.302) requires suitability reinvestigations every 5 years for personnel filling high risk positions. Additionally, the Department of the Interior Manual (441 DM 3) specifies that public trust positions (all positions that do not have national security related duties) must be designated at "risk levels commensurate with the public trust responsibilities and attributes of the position as they relate to the efficiency of the Federal service."

Cause:

Surface Mining did not have established policies and procedures for requiring background investigations for Federal and contractor personnel filling sensitive and critical public trust positions. In addition, Surface Mining did not include in two of the contracts we reviewed a requirement for contractor personnel to have background investigations.

Effect:

Without adequate security-related personnel policies and procedures, Surface Mining increases the risk that sensitive automated information systems operations and data could be impaired or compromised by Federal or contractor personnel.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel filling sensitive or critical public trust positions.
- 2. Ensure that all automated data processing contractor employees to have proper background clearances.
- 3. Ensure that periodic reinvestigations are completed every 5 years on personnel who are in public trust high risk positions.

Control Objective: The control objective for access controls is to limit or detect access to computer resources (for example, data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure.

D. Resource Classifications

Condition: Surface Mining had not classified its computer resources to determine the level

of security that should be provided.

Criteria: Office of Management and Budget Circular A-130, Appendix III, directs

agencies to assume that all major systems contain some sensitive information which needs to be protected but to focus extra security controls on a limited number of particularly high risk or major applications. Also, the Computer Security Act requires agencies to identify systems that process sensitive data.

Cause: Surface Mining did not have policies that provided for (1) information

resources to be classified, (2) resource classification categories to be based on the need for protective controls, (3) senior-level management to review and approve resource classifications, and (4) determinations of resource classifications to be documented. Additionally, classification of the information resources could not be achieved because a risk assessment (which identifies threats, vulnerabilities, and the potential negative effects that could result from disclosing confidential data or from not protecting the integrity of data supporting critical transactions or decisions) had not been performed on

the computer applications and systems software.

Effect: If information resources are not classified according to their criticality and

sensitivity, there is little assurance that Surface Mining is providing the most

cost-effective means to protect the computer resources.

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop and implement policies to classify Surface Mining's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A-1 30, Appendix III.

E. Access Levels

Condition:

Surface Mining did not have adequate controls in place to ensure that access levels granted to users of their automated information systems were appropriate. For example, we found that 14 personnel were granted "super-user" rights to the Fee Billing and Collection System (FEEBACS). Therefore, these users can manipulate FEEBACS databases, thus bypassing normal transaction processing controls.

Additionally, we found that access approval documentation was not available for all users on the systems. For example, based on a statistical sample of users selected for each of the operating and sensitive application systems reviewed, we found that access approval documentation was not available for:

- 20 (100 percent) of the users of the Novell operating system.
- 63 (80 percent) of 78 of the users of the Sun Solaris operating system.
- 3 1 (88 percent) of 35 of the users of the Windows NT operating system.
- 18 (16 percent) of 109 of the users of the financial system application.
- 20 (66 percent) of 30 of the users of FEEBACS application.

In addition, we found that access granted to users of these systems had not been approved by the system owners or managers and that periodic reviews had not been performed to determine who the users were and whether the levels of access granted in the automated information systems were appropriate. We also found that individuals whose employment had been terminated had access to the systems.

Criteria:

The National Institute of Standards and Technology's "Generally Accepted Principles and Practices for Securing Information Technology Systems" states:

Organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access. ... Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions . . . [and] it is necessary to periodically review user account management on a system. Reviews should examine the levels of access

each individual has, conformity with the concept of least privilege, whether all accounts are still active, [and] whether management authorizations are up-to-date.

The Department of the Interior Manual (375 DM 19, "Information Technology Security"), states, "Since the greatest threat to most computer systems comes from authorized users, bureaus should institute personnel controls such as least privilege, separation of duties, and individual accountability." Further, the Manual states, "Detailed procedural guidelines will be established ... to ensure IT [information technology] resources are properly protected and used only by authorized personnel."

Cause:

Surface Mining management had not established policies to implement a process of approving access to its automated information systems. In addition, there was no formal assignment of responsibility for approving systems access and for periodically reviewing access levels granted to system users. Also, procedures had not been implemented to ensure that system administration personnel were promptly notified of changes in employee assignments or employment terminations.

Effect:

As a result, there was a risk that unauthorized access, data manipulation, and disclosure of sensitive information may occur and that the unauthorized access would not be detected or detected timely.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Institute a policy of "least privilege" access levels to ensure that access to resources and data is limited to those users who require such access.
- 2. Develop and implement policies and procedures for approving access to the automated information systems that include the formal assignment of responsibility for approving systems access.
- **3.** Develop and implement procedures to ensure that user access levels are periodically reviewed to ensure that the current access provided is appropriate.
- **4.** Develop and implement procedures to ensure that system administration personnel are promptly notified of changes in employee assignments or employment terminations.
- 5. Implement controls to ensure that system owners approve all access to their applications in accordance with Surface Mining policy.

F. System Log-in

Condition: The number of unsuccessful log-in attempts to access Surface Mining's automated information systems exceeded the standard established by the Department. Specifically, we found that:

- Windows NT users were allowed unlimited unsuccessful log-in attempts. However, during our review, Surface Mining officials temporarily changed the setting to nine, with plans to change the setting to the standard of three attempts.
- Sun Solaris system users were allowed five unsuccessful log-in attempts before their user identifications (ID) and passwords were revoked,
- Financial system users were allowed eight unsuccessful log-in attempts before their user IDs and passwords were revoked. However, during our review, Surface Mining officials implemented new software and reduced the setting to the standard of three.

Additionally, the system log-in warning message that is used to warn potential unauthorized users that prosecution may occur was not displayed until after the user had logged on to the system and was authenticated as a valid system user.

Criteria:

The Department of the Interior's "Automated Information Systems Security Handbook" states that "unsuccessful attempts to enter a password should be limited to three attempts." Further, the "Handbook" requires that all communications equipment capable of displaying system messages display, as the first message seen by a user, a warning message regarding unauthorized use of Government computers and/or software.

Cause:

Although two of the three system administration personnel changed the number of log-in attempts, Surface Mining management had not developed polices and procedures that would implement the minimum standards established by the Department throughout Surface Mining. Additionally, Surface Mining management had not ensured that the warning message for unauthorized use was displayed as the first screen seen by a user.

Effect:

Without adequate controls in place to ensure proper access to automated information systems, there is the risk that unauthorized access to the systems could occur, resulting in the corruption of sensitive data or systems processing and the denial of service.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Develop and implement policies and procedures establishing the maximum number of log-in attempts allowed for its automated information systems in compliance with Department of the Interior regulations.
- 2. Ensure that the systems log-in warning message is the first screen displayed upon initial access and prior to the user being authenticated as a valid system user.

G. Password Settings

Condition: Password requirements for accessing Surface Mining's automated information systems were inadequate. Specifically, we found that:

- Passwords did not contain a minimum number of characters or include special characters.
- Passwords were fewer than the Department's standard of six characters in length, were common words, and were the same as users' IDs.
 - Passwords were not changed periodically.
 - Users were allowed to bypass password length and expiration settings.
- System administration passwords were shared. In one instance, the Sun Solaris operating system was accessed over the Internet using the system administration account and password, and the password was in an unencrypted form

Furthermore, using intrusion detection software, passwords for the Sun Solaris and Windows NT operating systems and the network router were identified within a 24-hour period, and powerful system administration level account passwords were obtained.

Criteria:

The National Institute of Standards and Technology's "Generally Accepted Principles and Practices for Securing Information Technology Systems" states that if passwords are used for authentication they should have attributes such as a minimum length of six characters, should include special characters, should not be in an online dictionary, and should be unrelated to the user ID. Also, the Department of the Interior's Automated Information Systems Security Handbook requires that passwords be a minimum of six characters and be changed periodically (90 days is recommended).

Cause:

Surface Mining had not developed policies and procedures on creating and changing passwords for its automated information systems. In addition, Surface Mining had not developed a policy requiring system administration personnel to log on to the system under specific user IDs that were issued to each individual.

Effect:

The current password settings reduce the effectiveness of the password as a control, thereby increasing the risk for unauthorized access to sensitive information through password disclosure.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Develop and implement password policies and procedures. In addition, controls to ensure compliance with these policies and procedures should be implemented.
- **2.** Implement a policy requiring system administration personnel to log on to the automated information systems under specific user IDs.
- **3.** Evaluate current capabilities and implement procedures to address encryption or other security methods to help prevent powerful system passwords and accounts from being compromised when traveling across a network, such as the wide area network and the Internet.

H. Novell Network Access

Condition:

"Public" users had inappropriate access to computer resources on the Novell network. Specifically, "Public" users had browse access at the root,* which allowed anyone to view user IDs and gather information without logging onto the network. Also, we identified 13 accounts with null³ passwords. In addition, the passwords were not required to be reset, which allowed anyone to log into these accounts to make unauthorized modifications or to manipulate data.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. The Circular defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." Also, the National Institute of Standards and Technology's "Generally Accepted Principles and Practices for Securing Information Technology Systems" states, "Organizations should implement logical access control based on policy made by a management official responsible for a particular system, application, subsystem, or group of systems."

Cause:

Surface Mining management had not developed policies and procedures to ensure that only authorized users had root access and that all accounts had active passwords.

Effect:

As a result, Surface Mining could not protect the Novell network operating system and other system software from unauthorized modification or manipulation and therefore could not ensure the integrity and availability of the network, the systems, and the data.

^{&#}x27;Root provides "a person with unlimited access privileges who can **perform** any and all operations on the computer. Also called superuser." (The Computer Language Company, Inc., <u>Computer Desktop Encyclopedia</u>, 1981-1998)

^{&#}x27;Null (null value) is "a value in a field or variable that indicates nothing was ever derived and stored in it." (The Computer Language Company, Inc., Computer Desktop Encyclopedia, 1981-1998)

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop policies and procedures to ensure that controls are in place to protect the Novell network operating system and other system software from unauthorized modification or manipulation.

I. User Access Control

Condition: Surface Mining's Information Systems Management Office in Washington, D.C., and the Division of Financial Management in Denver, Colorado, had not implemented controls that limited access to its Novell file servers. Specifically, the "SECURE CONSOLE" command for the Novell file servers was not used. The "SECURE CONSOLE" command removes DOS from the file servers, which prevents users from shutting down the file server, exiting to DOS, and running unauthorized programs. Also, the "LOCK CONSOLE" command was not used. The "LOCK CONSOLE" command ensures that only users with proper authorization can access the file servers. Additionally, the password for the "RCONSOLE" was not encrypted and resided in at least two files (the autoexec.ncf and the netinfor.cfg) at the Division of Financial Management. The "RCONSOLE" command establishes connections that enable keyboard strokes at the workstations to be sent to the file servers and screen image changes at the file servers to be sent to remote workstations.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Circular A-130 defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

Cause:

Surface Mining management had not identified or implemented the technical controls necessary to ensure that only authorized users had access to the Novell file servers.

Effect:

As a result, Surface Mining increased the risk that unauthorized individuals could access its file servers to run programs or gain access to data files. For example, because the "RCONSOLE" command was not encrypted, sensitive files could be copied to an unprotected location during maintenance/emergency procedures or be viewed by technical contractors or staff who had temporary supervisory access to the file servers.

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, identify and implement the technical controls necessary to ensure that only authorized users

⁴Encrypt is to "encode data for security purposes." (The Computer Language Company, Inc., <u>Computer</u> Desktop Encyclopedia, 1981-1998)

have access to the Novell file servers. The controls should include using the "SECURE CONSOLE" command in the autoexec.ncf file, encrypting the "RCONSOLE" password, and using the "LOCK CONSOLE" command.

J. Network Protection

Condition:

Surface Mining's Division of Financial Management did not protect its local area network against probes and attacks from unauthorized users. Specifically, the configuration of the Division's network allowed internal and external users to access the systems.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Circular A-130 further defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." Additionally, the National Institute of Standards and Technology's "Executive Guide to the Protection of Information Resources" states, "Agency information should also be protected from intruders... as well as from employees with authorized computer access privileges who attempt to perform unauthorized actions."

Cause:

The Division of Financial Management did not protect its local area network because it had not implemented a firewall⁵ system that defined the services and accesses to be permitted or denied when accessing its local area network. Although the Division had a router in place, the router was not used as a firewall to filter access.

Effect:

As a result, unauthorized users could easily gain access to the Division of Financial Management's financial and other sensitive applications. For example, the Division's network was vulnerable to passive threats, such as an intruder viewing data, and active threats, such as an intruder modifying data.

⁵Firewall is a "method for keeping a network secure. It can be implemented in a **single** router that filters out unwanted packets, or it may be a combination of technologies in router and hosts. They are also used to keep internal network segments secure. For example, a research or accounting **subnet** might be vulnerable to snooping from within." (The Computer Language Company, Inc., <u>Computer Desktop Encyclonedia</u>, 1981-1998)

⁶Router is a "device that forwards data packets from one local area network or wide area network to another. Routers are used to segment local area networks in order to balance traffic within workgroups and to filter traffic for security purposes and policy management." (The Computer Language Company, Inc., <u>Comnuter Desktop Encyclonedia</u>, 198 1- 1998)

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, install a firewall system for the Division of Financial Management's local area network.

SYSTEM SOFTWARE CONTROLS

Control Objective: The control objective for system software is to limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.

K. System Audit Tools

Condition: Surface Mining management did not use available system audit tools to ensure integrity over automated information systems processing and data and to detect inappropriate actions by authorized users. For example, we found that:

- Systems audit software was not used for the Windows NT and Novell servers and the Hewlett Packard and Sun Solaris operating systems at the Divisions of Information Systems Management and Financial Management. According to the "NIST Handbook," this type of tool could assist data center and installation security management in evaluating its systems for security flaws, such as identifying security exposures related to "improper access controls or access control configurations, weak passwords, lack of integrity of the system software, or not using all relevant software updates and patches."
- Some systems options for the Windows NT servers and the Novell operating system at the Divisions of Information Systems Management and Financial Management that produce audit trails in the systems were not implemented. However, for those systems that had systems options implemented to produce audit trails, the audit trails were not reviewed periodically. In addition, in the systems that had implemented the options to maintain the audit trail, the settings allowed the systems to overwrite* the audit trail. Therefore, in some of the systems, an audit trail that logs the results of actions taken by system programmers, system administration, and system users could not be reviewed.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, Circular A- 130 states that individual accountability is one of the personnel controls required in a general support system. Circular A- 130 further states that an example of one of the controls to ensure individual accountability is examining or looking at patterns of users' behavior by reviewing the audit

^{&#}x27;Overwrite is "to record new data on top of existing data such as when a disk record or file is updated." (The Computer Language Company, Inc., Computer Desktop Encyclopedia ,1981- 1998)

SYSTEM SOFTWARE CONTROLS

trails. Also, the "NIST Handbook" states that audit trails are a technical mechanism to achieve individual accountability. In addition, the "Handbook" recognizes that not taking advantage of automated tools to assist in the review of computer systems security features "puts system administrators at a disadvantage."

Cause:

Surface Mining management did not (1) require systems integrity and verification software, (2) implement systems options to record actions taken affecting systems controls and processing, (3) use and maintain available systems audit trails to detect and identify inappropriate actions affecting the systems processing and data integrity, and (4) establish procedures requiring periodic reviews of resultant systems logs.

Effect:

As a result, inappropriate systems settings and processing were not identified and recorded. Additionally, without periodic reviews of system audit trails, there was an increased risk that processing problems or unauthorized activities would not be detected or would not be detected timely and that the individual responsible would not be held accountable for the inappropriate actions.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- Evaluate acquiring systems verification and auditing software.
- 2. Implement the systems options available in each of the operating systems to record activities affecting the systems.
- **3.** Implement policies and procedures to ensure that systems logs are used and are maintained for an appropriate amount of time to provide an adequate audit trail of systems activities and are controlled by personnel independent of the systems access control administration function.
- 4. Develop and implement procedures to ensure that periodic reviews of systems logs for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Surface Mining management.

SYSTEM SOFTWARE CONTROLS

L. System Software Vulnerabilities

Condition: Surface Mining did not have adequate controls to ensure that necessary system software updates were implemented in a timely manner. Specifically, service packs⁹ available in October 1998 to address vulnerabilities in the Windows NT operating system had only been implemented by the Division of Financial Management in two of the four NT systems affected by the vulnerabilities as of March 30, 1999.

Criteria:

Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," states that "software maintenance is the performance of those activities required to keep a software system operational and responsive after it is accepted and placed into production." In addition, the "Guideline" states that "software maintenance is the set of activities which result in changes to the originally accepted (baseline) product set." Further, the "Guideline" states that "these changes are made in order to keep the system functioning in an evolving, expanding user and operational environment."

Cause:

Surface Mining management had not established policies and procedures to ensure that current service packs to the operating systems were evaluated for implementation and that the current fixes available from the vendor to address systems problems and vulnerabilities were implemented when necessary.

Effect:

The risk is increased that known operating systems vulnerabilities that have been identified and addressed by the systems software vendor will not be implemented by Surface Mining management as necessary.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Establish policy and procedures for ensuring that available software updates and service packs are reviewed to identify those that should be implemented to address an applicable systems vulnerability.
- 2. Implement procedures to ensure that those updates which are determined to be needed are implemented in a timely manner.

⁹Service packs is "a software patch that is applied to an Installed application. It is typically downloaded from the vendor's Web site. When executed, it modifies the application in place." (The Computer Language Company, Inc., Desktop Encyclopedia, 1981-1998)

SEPARATION OF DUTIES

Control Objective: The control objective for separation of duties is the establishment of policies, procedures, and organizational structure so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.

M. Duties Related to Automated Information Systems

Condition: The duties related to all the automated information systems throughout Surface Mining were not separated effectively. Specifically, we found that:

- Individuals responsible for setting up users of the automated information systems were also the individuals controlling the systems security logs that record the activities of the users of these systems.
- Individuals who controlled systems audit trails were also responsible for system administration, which resulted in these personnel monitoring their own system activities.
- Application programmers who made code changes to software were also responsible for moving those changes into production.
- Application programmers were responsible for changing production data.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires that security controls of personnel include separation of duties. Circular A- 130 and the "NIST Handbook" define separation of duties as the division of roles and responsibilities and of steps in a critical function so that no one individual can undermine a critical process. Additionally, Surface Mining's Information Resources Management (IRM) Policies and Procedures Manual states that appropriate safeguards should be used "to prevent unauthorized access to and use of information, data, and software." The "Generally Accepted Principles and Practices for Securing Information Technology Systems," issued by the National Institute of Standards and Technology, states, "In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification." This publication further states that "access to online audit logs should be strictly controlled" and that "organizations should strive for separation of duties between security personnel who administer the access

SEPARATION OF DUTIES

control function and those who administer the audit trail." Additionally, the publication states that "audit trails should be reviewed periodically."

Cause:

Surface Mining management had not ensured that personnel whose duties included performing reviews of security logs were different from the personnel whose responsibilities included establishing users on those systems. In addition, no policy had been implemented to ensure that systems audit trails were maintained and controlled by individuals other than those individuals responsible for administration of the access control function. Further, the Division of Financial Management did not appropriately assign duties for application programmers to ensure that critical processes were not subverted. Specifically, application programmers should not have access to production data because production data should be restricted to users.

Effect:

Since logging and subsequently reviewing the logs are primary detection controls used to identify inappropriate activities of users who have significant system access, separating these two functions provides one of the main internal controls over the system administration function. As a result, there was an increased risk that inappropriate actions by the individuals who established system users would not be detected or would not be detected timely. In addition, there is an increased risk that accidental or intentional unauthorized actions by programmers could threaten the integrity of Surface Mining's data and disrupt systems processing.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Implement procedures to ensure that personnel who perform access control administration are not the same individuals who review and control systems security logs and systems audit trails.
- 2. Implement controls to ensure that application programmers are not responsible for moving changed software into the production environment and do not have access to update/change production data.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT"

Control Objective: The control objective for software development and change management is to prevent unauthorized programs or modifications to an existing program from being implemented.

N. Change Management Controls

Condition: Change management controls over applications software were not adequate. Specifically, we found that:

- The applications implementation, conversion, and testing process was inadequate, causing data to be incorrect and requiring users to identify data errors, prepare and submit change requests to correct the data, and to reenter the correct data. Additionally, without adequate change management controls, Surface Mining was at risk of having malicious codes inadvertently or deliberately added to the applications software.
- Software edits were removed without ensuring that change management controls were followed. Thus, changes were made that were not authorized, approved, and tested.
 - User change requests were not addressed in a timely manner.

Criteria:

Office of Management and Budget Circular A-127, "Financial Management Systems," states, "Financial management systems shall be designed to provide for effective and efficient interrelationships between software, hardware, personnel, procedures, controls, and data contained within the system." Surface Mining's "Information Resources Management (IRM) Policies and Procedures Manual" requires system owners to establish formal, written standards for program changes (both scheduled and emergency) and to authorize all scheduled program changes. In addition, the "Manual" requires system managers to ensure that all program changes meet formal, written standards and to notify the system owner when emergency program changes are made. Also, the "Manual" requires that unit, integration, system, and acceptance testing be used when a new system is developed or an existing system is enhanced.

Cause:

Surface Mining management did not ensure that its "Information Resources Management (IRM) Policies and Procedures Manual" was followed for changing applications software. Additionally, because change requests were not addressed timely, Surface Mining had a significant change request backlog that may reduce the ability of the applications meeting the users' requirements.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

Effect:

As a result, the risk was increased that processing irregularities or malicious codes could be introduced, data lacked integrity, and applications were not functioning to meet users' needs. In addition, the applications did not process data accurately, which resulted in insufficient and costly manual processes, such as time and personnel resources, to supplement the applications deficiencies.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Enforce Surface Mining's written policies and procedures to ensure that all application programs and modifications are properly authorized, tested, and approved and that access to and distribution of programs is controlled.
- 2. Establish the process of correcting applications deficiencies as a high priority to reduce manual processes.
- **3.** Review change requests timely to ensure that user requirements are supported in the applications.

Control Objective: The control objective for service continuity is to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

0. Business Continuity of Operations

Condition: Surface Mining had not developed continuity of operations plans for its telecommunications links or finalized plans for its facilities and data centers. In addition, while Surface Mining had completed draft plans for its data centers and its facilities, these plans had not been approved or tested, and training had not been provided to personnel on the plans. Further, the off-site facility (cold storage for backup tapes) for Surface Mining headquarters operations was not located at. least 1 mile from the headquarters location.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish a comprehensive contingency plan and periodically test the capability to perform the agency function supported by the application, as well as critical telecommunications links, in the event of a disaster or system Additionally, the "NIST Handbook" states that a comprehensive disaster recovery plan is necessary to ensure the timely recovery of all business functions and the systems environment that are critical for day-to-day operations and to minimize downtime. Further, the "NIST Handbook" recognizes that personnel should be trained in their contingency-related duties. In addition, the "NIST Handbook" states that a primary contingency strategy for applications and data is storage at a secure off-site facility. According to the "NIST Handbook," a secure off-site storage facility should be physically and environmentally protected to prevent unauthorized individuals from access and to protect data from heat, cold, or harmful magnetic fields and should be located at least 1 mile from the installation. Also, the Department of the Interior "Automated Information Systems Security Handbook" mandates off-site storage for "all AIS [automated information systems] installations providing critical support to the organization's missions."

Cause:

Prior to the issuance of the Department of the Interior's Office of Managing Risk and Public Safety Policy Bulletin 98-001, "Continuity of Operations Planning - Guidance and Schedules," dated March 1998, Surface Mining did not have any contingency plans for its telecommunications links, facilities, or data centers. At the time of our review, Surface Mining had developed contingency plans for its data centers and facilities, but it had not included plans for telecommunications links and had not addressed the testing of these plans. Further, Surface Mining management was unaware of the requirement

to have an off-site storage facility located at least 1 mile from the original computer facility installation.

Effect: As a result, Surface Mining increased its risk of being unable to recover and resume critical operations should the systems fail or disasters occur.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

- 1. Ensure that a contingency plan is developed for critical telecommunications links.
- 2. Ensure that contingency plans for telecommunications links, facilities, and the data center are finalized and tested and that test results are used to update these plans. Additionally, assurance should be provided that personnel are trained to implement the plans.
- **3.** Provide for a secure off-site storage facility that is at least 1 mile from the computer facility.

P. Incident Response Plan and Team

Condition: Surface Mining did not have a formal incident response plan and a formal response team in place to respond timely and efficiently to information system security incidents whether an incident was caused by a computer virus, other malicious codes, or a system intruder (either an insider or an outsider). A security incident may affect sensitive systems at different network sites, including contractors and clients. For example, end users would not know whom to contact if they find or have inadvertently introduced a virus to the network. Further, the system administrators may not escalate the incident to Surface Mining's security management, thus allowing the virus to populate the wide area network.

Criteria:

Office of Management and Budget Circular A-130, Appendix III, states that "when faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms."

The National Institute of Standards and Technology's "Generally Accepted Principles and Practices for Securing Information Technology Systems" states that "an organization should address computer security incidents by developing an incident handling capability."

Cause:

Surface Mining did not have a formal incident response plan or a formal response team because management believed that the local area and wide area network administrators were prepared to respond to each security breach based on what occurred during the incident. We believe that without a formal plan, Surface Mining may not have identified all types of incidents and actions to take to prevent further spreading of a virus. A formal incident response plan would include, for example, names of important contacts, both external and internal, such as managers and technical support personnel to aid in containment and recovery efforts and, if appropriate, Federal law enforcement officials to investigate the incidents.

Effect:

Without a formal response plan and team, Surface Mining cannot provide assurance to its users, contractors, or clients that data would be protected, that security incidents would be handled quickly and efficiently, and that corrective actions would be implemented.

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop and implement a formal incident response plan and team.

OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT SENSITIVE AUTOMATED INFORMATION SYSTEMS

Office of Surface Mining's Sensitive Automated Information Systems as Reported to the Department of the Interior in Surface Mining's "Automated Information Systems Security Plan," Dated February 1998

Advanced Budget/Accounting Control and Information Systems (ABACIS)

Audit Fee Billing and Collection System (AFBACS)

Abandoned Mine Lands Inventory System (AMLIS)

Applicant Violator System (AVS)

Civil Penalty Accounting Control System (CPACS)

Coal Data Repository System (CDR)

Electronic Mail (E-Mail)

Fee Billing and Collection System (FEEBACS)

Grants Information Fund Tracking System (GIFTS)

Litigation Tracking System (LTS)

Payroll/Personnel Data Entry (PAY/PERS)*

Synergistic Acquisition Tracking Inventory Network (SATIN)

Technical Information Processing System (TIPS)

Additional Sensitive Systems**

Correspondence Tracking System (CTS)

Office of Surface Mining Wide Area Network (OSMNET)

Work Assignment Tracking System/Mine Information, Project Planning System (WATTS/MIPPS)

Administrative Records Management System (ARMS)

^{*}In its response to the draft report, the Office of Surface Mining stated that this system "is no longer used."

^{**}In its response to the draft report, the Office of Surface Mining identified additional mission critical or sensitive systems.

OFFICE OF SURFACE MINING RESPONSE TO IG AUDIT RECOMMENDATIONS September 17, 1999

OSM reviewed the Draft Audit Report and agrees that we must have documented security plans, risk analysis, and a security policy. Although many of our security procedures were not written in these specific documents, we do have security controls in place. The Division of Financial Management operates sensitive systems which process financial data. These systems are comprised of two computer platforms, the Hewlett-Packard and the SUN, which operate seven of the 16 Mission Critical Systems in OSM.

To ensure that the operating environment at the Division of Financial Management is secure and that the financial systems are protected, we maintain a secure building that houses the computer systems. The computer room contains an un-interruptible power supply and is environmentally controlled with an "automated notification" temperature and electrical monitor. In addition, we have off-site storage of system and application back-ups which have been tested,

Security access systems are in place that limit "system administrator" privileges to the system administrator, their backup, and select other personnel on an as needed basis. We have separation of functional duties to preclude any one person from processing a transaction from beginning to end. In addition, Daily Synchronization Reports are produced to test the integrity of the data in the systems and all system modifications are tested prior to implementation.

The following responses address each of the 38 recommendations identified in Appendix 1 of the Draft Audit Report:

SECURITY PROGRAM

A. Risk Assessments

Recommendations:

1. Determine the risks associated with each of the systems and, based on the results of the risk assessments, establish appropriate security policies and procedures.

Response: OSM concurs with tliis recommendation and offers the following response:

OSM completed a risk assessment for each of its 16 mission critical systems and has established security policies and procedures. The risk assessments for each of the OSM's mission critical systems are at attachment I. The security policies and procedures are at attachment II.

2. Ensure that risk assessments are conducted in accordance with Federal guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the risk assessments should address significant risks affecting sensitive systems and major applications, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of residual risk.

Response: OSM concurs with this recommendation and offers the following response:

The risk assessments developed by OSM, were conducted in accordance with Federal Guidelines and document the acceptance of risk and the selection of appropriate controls. A copy of these risk assessments are at attachment I. The IG has conducted an interim review of several of these risk assessments and given OSM recommendations for improvements, and these recommendations are being incorporated into the completed final risk assessments.

3. Formally assign and communicate responsibility to those required to participate in assessing risks.

Response: OSM concurs with this recommendation and offers the following response:

The Information Systems Security Officer (ISSO) has been formally assigned as the security officer for OSM, and is responsible for ensuring that continuing risk assessments are performed on OSM's mission critical systems. The Information System Security Officer has contacted each of the systems owners of OSM's 16 mission critical systems and had them participate in developing the risk assessments at attachment I. Chapter I of the Security Directive provides policy concerning the Program Managers responsibility for creating and implementing security plans and risk assessments for mission critical systems in their area of responsibility.

SECURITY PROGRAM

B. System Security Plans

Recommendations:

1. Provide resources to ensure that automated information systems security plans are developed for its general support systems and major applications in accordance with the Computer Security Act; Office of Management and Budget Circular A-130, Appendix III; and the National Institute of Standards and Technology Special Publication 800-18.

Response: OSM concurs with this recommendation and offers the following response:

OSM has provided the necessary resources and developed system security plans for each of its mission critical systems. The security plans for each of OSM's 16 mission critical systems are at attachment III. There is one automated system on your list of mission critical systems that should be removed. The Payroll/Personnel Data Entry (PAY/PERS) is no longer used by OSM. The IG conducted an interim review of several of these security plans and has given OSM recommendations for improvements. These recommendations are being incorporated into the completed security plans.

2. Ensure that the automated information systems security function is elevated organizationally to report directly to Surface Mining's Chief Information Officer and formally provide the position with the authority to implement and enforce the Surface Mining-wide computer security program.

Response: OSM concurs with the recommendation that the security function should be elevated, however we feel that it should be elevated to the Deputy Chief Information Officer rather than the Chief Information Officer, for the following reason:

The Deputy Director of OSM is designated as Chief Information Officer for the Bureau. *However*, at the present time, OSM does not have a Deputy Director. Therefore, OSM will elevate the security function organizationally to report directly to the Deputy Chief Information Officer.

3. Report the lack of security plans for surface mining's 13 sensitive systems as material weakness in Surface Mining's annual assurance statement on management controls for fiscal year 1999.

Response: OSM concurs with the finding that there was a lack of security plans for 13 sensitive systems. However, OSM does not feel that this should be reported as a material weakness in the annual assurance statement on management controls for fiscal year 1999, for the following reason:

OSM has completed security plans for all of it's 16 mission critical systems. These security plans are at attachment III.

SECURITY PROGRAM

c. Security-Related Personnel Policies and Procedures

Recommendations:

1. Ensure that personnel security policies and procedures are developed, implemented and enforced, including those for obtaining appropriate security clearances for personnel filling sensitive or critical public trust positions.

Response: OSM concurs with this recommendation and offers the following response:

OSM has developed a Security Directive (copy at attachment II), which contains personnel security policies and procedures for obtaining appropriate security clearances for personnel filling sensitive and critical trust positions. In addition, the Office of Personnel has developed a procedures guidelines document, which has been included in Chapter VI of the Security Directive, that will provide guidance on how to designate position sensitivity for all OSM positions, and the level of background investigations which should be completed on each type of position.

The Office of Personnel is in the process of identifying all personnel in Sensitive Computer Areas and their position risk designation to assure proper clearance and background investigations are completed. The procedures for implementing this policy is found in Chapter VI of the Security Directive.

2. Ensure that all automated data processing contractor employees have proper background clearances.

Response: OSM concurs with this recommendation and offers the following response:

OSM has developed mandatory language to be used in all agency contracts requiring that all contractor employees receive proper background clearances. This language will be in all agency contracts effective with contract renewals for October 1, 1999. In addition to mandatory language in all agency contracts, all contractors currently on-board will receive a background clearance, if required, and the requirement for all new contractor employees to receive proper background clearances is included in the OSM Security Directive at attachment II, in Chapter I, Section E.

3. Ensure that periodic re-investigations are completed every 5 years on personnel who are in public trust high risk positions.

Response: OSM concurs with this recommendation that periodic re-investigations should be completed on personnel in public trust high risk positions and offer the following response:

OSM agrees that re-investigations should be completed on personnel in public trust high risk positions. Although we are a small agency with few resources for re-investigations, we will ensure that periodic re-investigations are completed every five years on personnel in public trust high risk positions. Chapter VI contains policy on OSM's Personnel Security Program.

ACCESS CONTROLS

D. Resource classifications

Recommendation:

1. We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop and implement policies to classify Surface Mining's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A-130 Appendix III,

Response: OSM concurs with this recommendation and offers the following response:

OSM has completed risk analyses and security plans for all sensitive systems, which will be approved by appropriate agency personnel in concert with Program Managers. The Security Directive at attachment II includes policy on how to designate sensitive data and requirements for sensitive and non-sensitive data. In addition, OSM has developed and implemented policies in the OSM Security Directive to ensure that access controls are in place that limit access to Sensitive Computer Areas to protect computer resources from unauthorized modifications, loss, disclosure or compromise.

E. Access Levels

Recommendations:

1. Institute a policy of "least privilege" access levels to ensure that access to resources and data is limited to those users who require such access.

Response: OSM concurs with this recommendation and offers the following response:

In Chapter XII, Section D of OSM's Security Directive, at attachment II, policy has been included to ensure that access to resources and data is limited to those users who require such access. The Division of Financial Management completes a total review of all User access privileges every six months. This involves the system owners reviewing all employees who have access to their applications and related assigned privileges.

2. Develop and implement policies and procedures for approving access to the automated information systems that include the formal assignment of responsibility for approving sys tern access.

Response: OSM concurs with this recommendation and offers the following response:

OSM has written policies and procedures in Chapter XII, Section D of the Security Directive for approving access to the automated information systems and has assigned responsibility for approving systems access to the appropriate areas within the organization. OSM requires that all requests for User ID's and access privileges by DFM users be documented

via a hardcopy authorization form or electronic request with proper approval by system owners.

3. Develop and implement procedures to ensure that user access levels are periodically reviewed to ensure that the current access provided is appropriate.

Response: OSM concurs with this recommendation and offers the following response:

OSM has included procedures in Chapter XII, Section D of the Security Directive that user access levels are periodically reviewed to ensure that access levels provided are appropriate. OSM requires that all system administrators complete a total review of all User access privileges every six months. This involves the system owners reviewing all employees who have access to their applications and related assigned privileges.

4. Develop and implement procedures to ensure that system administration personnel are promptly notified of changes in employee assignment or employment terminations.

Response: OSM concurs with this recommendation and offers the following response:

The OSM Employee Exit Clearance Form will be updated to include a section for the supervisor of the employee being reassigned or terminated to sign. The signature will remind the supervisor of his responsibility to immediately notify the Information Systems Security Officer that a particular employee has had a change of status. In addition, as an increased security precaution, the Office of Personnel will send a message to the systems administrators listing all employees that have left the agency during the previous pay period. This policy is in Chapter IX, Section B.

5. Implement controls to ensure that system owners approve all access to their application in accordance with Surface Mining Policy.

Response: OSM concurs with this recommendation and offers the following response:

The OSM Security Directive, attachment II, Chapter IX, Section B, contains policy requiring system owners to approve all access to their application systems. OSM requires that all requests for User ID's and access privileges be documented via a hardcopy authorization form or electronic request with proper approval by system owners. Before user-id's generated as a result of these requests are activated, DFM must receive a signed "Rules of Behavior" from the user.

F. System Log-in

Recommendations:

Develop and implement policies and procedures establishing the maximum log-in attempts allowed for it automated information systems in compliance with Department of Interior regulations.

Response: OSM concurs with this recommendation and offers the following response:

OSM has implemented policy in its Security Directive that establishes the maximum unsuccessful log-in attempts to be three (3) before the user is locked out of the system. However, the SUN computer at DFM is set for five (5) attempts prior to invalidation of a User ID, because this is a standard for the SUN Solaris System. This policy is in Chapter XII, Section D.

2. Ensure that the systems log-in warning message is the first screen displayed upon initial access and prior to the user being authenticated as a valid system user.

Response: OSM concurs with the recommendation and offers the following response:

The hardware and operating system architecture of the systems does not always allow a warning message to be the first screen displayed upon initial access to the system. However, OSM will place systems log-in warning message as close to the first screen as the hardware and software will allow.

G. Password Settings

Recommendations:

1. Develop and implement password policies and procedures. In addition, controls to ensure compliance with these policies and procedures should be implemented.

Response: OSM concurs with the recommendation and offers the following response:

OSM has included password policy and other access control measures in the Security Directive. The policy requires a minimum of six alphanumeric characters on passwords. The system software has been modified to not accept a password of less than the minimum required characters. This policy is in Chapter XII, Section B of the Security Directive.

2. Implement a policy requiring system administration personnel to log on to the automated information systems under specific user **ID's**.

Response: OSM concurs with the recommendation and offers the following response:

The OSM Security Directive, at attachment II, contains policy requiring system administrators to have and use their own unique password when logging into the systems as an administrator. This policy specifically states that system administrators are not to share

passwords. In addition, the policy states that passwords will be changed every 90 days . This policy is in Chapter XII, Section B of the Security Directive.

3. Evaluate current capabilities and implement procedures to address encryption or other security methods to help prevent powerful system passwords and accounts from being compromised when traveling across a network, such as the wide area network and the internet.

Response: OSM concurs with the recommendation and offers the following response:

Upon implementation of the Firewall at DFM during the fall of 1999, encryption software will be installed on client work stations belonging to the various System Administrators within the DFM to provide increased security for their user id's and passwords during transmittal.

H. Novel Network Access

Recommendation:

1. We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop policies and procedures to ensure that controls are in place to protect the Novell network operating systems and other system software from unauthorized modification or manipulation.

Response: OSM concurs with this recommendation and offers the following response:

OSM has included policy in the Security Directive to ensure that users are not given inappropriate access to computer resources on the Novell network. Users will not be given browse access at the root, and the Security Directive (copy at attachment II), will not allow the use of null passwords. This policy is in Chapter XII, Section D.

I. User Access Control

Recommendation:

1. We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, identify and implement the technical controls necessary to ensure that only authorized users have access to the Novell file servers. The controls should include using the "SECURE CONSOLE" command in the autoexec.ncf file, encrypting the "RCONSOLE" password and using the "Lock Console" command.

Response: OSM concurs with the recommendation that only authorized users should have access to the Novell file servers, and offers the following response:

1. The Security Directive will include policy that requires the use of encrypting the "RCONSOLE" password. In addition, the policy will also require that "SECURE CONSOLE" command in the autoexec.ncf file, and the "LOCK CONSOLE" command must be used, unless the computer room is secure, and unauthorized users are not able to gain access to the computer room. This policy is in Chapter XII, Section B.

J. Network Protection

Recommendations:

1. We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, install a firewall system for the Division of Financial Management local area network.

Response: OSM concurs with this recommendation and offers the following response:

A firewall is currently being installed at the Division of Financial Management in Denver, and in the Headquarters location in Washington, D.C.

SYSTEM SOFTWARE CONTROLS

K. System Audit Tools

Recommendations:

1. Evaluate acquiring systems verification and auditing software.

Response: OSM concurs with this recommendation and offers the following response:

OSM will establish a team from its group of Information Technology resources to evaluate acquiring systems verification and auditing software. This team will be established during the agency-wide IRM Coordinators meeting being conducted in November, 1999.

2. Implement the systems options available in each of the operating systems to record activities affecting the system.

Response: OSM concurs with this recommendation and offers the following response:

Both the SUN and HP computer systems at DFM maintain and retains system logs for a period of six months. The audit function on both NT and Novell in other locations are enabled.

3. Implement policies and procedures to ensure that system logs are used and are

maintained for an appropriate amount of time to provide an adequate audit trail of systems activities and are controlled by personnel independent of the systems access control administration function.

Response: OSM concurs with this recommendation and offers the following response:

Both the SUN and HP computer systems at DFM maintain and retains system logs for a period of six months. The audit function on both the NT and Novell servers in Washington are enabled.

4. Develop and implement procedures to ensure that periodic reviews of systems logs for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Surface Mining Management.

Response: OSM concurs with this recommendation and offers the following response:

System administrators/system managers will review logs periodically and report incidents in conformance with OSM's Incident Reporting Procedures. The Incident Reporting Procedures are in Chapter XI, Section G of the Security Directive.

L. System Software Vulnerabilities

Recommendations:

Establish policy and procedures for ensuring that available software updates and 1. service packs are reviewed to identify those that should be implemented to address and applicable systems vulnerability.

Response: OSM concurs with this recommendation and offers the following response:

OSM has established policy to ensure that available software updates and service packs are reviewed to identify needed software upgrades and new service packs. The DFM Quality Assurance Log schedules a monthly task to hardware system managers to check via the Internet for software upgrades and new service packs.

The system manager, based on their research and needs, will decide on implementing software upgrades. This policy is in Chapter XI, Section H of the Security Directive.

Implement procedures to ensure that those updates deemed needed are implemented 2. in a timely manner.

Response: OSM concurs with this recommendation and offers the following response:

The DFM Quality Assurance Log schedules a monthly task to hardware system managers to check via the Internet for software upgrades and new service packs. The system manager, based on their research and needs, will decide on implementing software upgrades. This policy is in Chapter XI, Section H of the Security Directive.

SEPARATION OF DUTIES:

M. Duties Related to Automated Information Systems

Recommendations:

1. Implement procedures to ensure that personnel who perform access control administration are not the same individuals who review and control systems security logs and systems audit trails.

Response: OSM concurs with the recommendation and offers the following response:

DFM has procedures in place to ensure that personnel who perform access control administration are not the same individuals who review and control systems security logs and systems audit trails. Procedures of this type are handled outside of the particular **software** system, because hardware and software providers (Hewlett-Packard, SUN, NOVELL, and NT included) established access to system security logs, system audit trails, and the ability to create and modify user access to their computer platforms as a function of the System Manager.

In order to better control these functions, DFM has implemented a number of "checks and balances" to ensure integrity. The establishment of a new user or the modification of an existing user must be requested by the users supervisor and approved by the system owner. Then, DFM's Information Systems Security Officer coordinates with the appropriate System Manager to create or modify the user's access to the system. Biannually, the system owners reviews a list of registered users and their access levels to confirm that they are valid. This creates both a "separation of duties" between those individuals who authorize access and those individuals who enable access to DFM systems and provides for a continuing re-evaluation of access to DFM systems.

With regard to the review of control systems security logs, system software monitors unauthorized access attempts to DFM systems, and automatically disables a user ID after three to five access attempts, depending on the system specifications. This software also maintain logs of successful access to DFM systems. Logs are also reviewed by the system owner and the Information Systems Security Officer periodically to determine if unauthorized access attempts to DFM systems are being attempted.

DFM defines systems audit trails as database logs. These database logs are controlled by

the individual database administrators. Database logs are used by DFM for two purposes: (1) to identify invalid or inappropriate changes to data within DFM systems, and (2) to recover data whenever a hardware or software error occurs. Because these logs are controlled by the-database administrator and not the System Manager, the requirement for separation of duties is satisfied.

2. Implement controls to ensure that application programmers are not responsible for moving changed software into the production environment and do not have access to update/change production data.

Response: OSM concurs with this recommendation and offers the following response:

DFM's computer programmers have the capability to check production software in and out of the application so&are libraries and to modify production data. This is a very typical process in small data processing shops. DFM does not have funding or staffing levels to maintain independent software librarians, security officers, security maintenance personnel and programmers who only work on test areas and do not have access to production areas.

Change control procedures are used by the system owner and technical staff in requesting and completing changes (STR and DSR). Programmers are assigned tasks, the systems owner tests the programmers modifications, and the programmer schedules and implements the modifications after a successful test and approval by the system owner. All program modifications are recorded via system logs, table/file date stamping, and in the DSR/STR System.

Quality and internal controls are completed via external reconciliation, quality assurance, internal control reports, and via separation of functional duties to preclude a transaction from being completed from beginning to end by one person.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

N. Change Management Controls

Recommendations:

1. Enforce Surface Mining's written policies and procedures to ensure that all application programs and modifications are properly authorized, tested, and approved and that access to and distribution of programs is controlled.

Response: OSM concurs with this recommendation and offers the following response:

OSM will enforce its policies and procedures to ensure that all application program modifications are properly authorized, tested, and approved and that access to and distribution of programs are controlled. This policy is in Chapter XII, Section H and Chapter IV, Section D of the Security Directive.

2. Establish the process of correcting applications deficiencies as a high priority to reduce manual processes.

Response: OSM concurs with this recommendation and offers the following response:

DFM has a process for prioritization of System Trouble Reports (STR) and Data System Request (DSR). All requests for changes to the systems are recorded on these forms, STR's are corrected immediately. DSR's are generated by users to improve reports, develop new reports, develop new modules, etc. We encourage users to prepare a DSR for all desired changes so that system owners can maintain an inventory of requested changes and prioritize the top five requests, Our current inventory is larger because of the resource drain by Year 2000, standard general ledger and budget object class changes.

The DFM Quality Assurance Log has an event scheduled every two weeks that requires a review and prioritization of STR/DSR. This process to correct deficiencies will be established as a high priority.

3. Review Change request timely to ensure that user requirements are supported in the applications.

Response: OSM concurs with this recommendation and offers the following response:

The DFM Quality Assurance Log has an event scheduled every two weeks that requires a review and prioritization of STR/DSR. This process to correct deficiencies will be established as a high priority. OSM will provide timely review of change request to ensure that user requirements are supported in a timely manner.

SERVICH INUITY

0. Business Continuity of Operations

Recommendations:

1. Ensure that a contingency plan is developed for critical telecommunications links.

Response: OSM concurs with the recommendation and offers the following response:

OSM has developed a Continuity of Operations Plan (copy at attachment VI), which documents the re-establishment of critical telecommunications services, including telecommunications data links, within "Appendix F", Telecommunications Services. For example, DOINET, FTS2000 (AT&T), FTS2001 (MCI-Worldcorn), and the General Services Administration's local exchange carriers' service contracts stipulate loss-of-service recovery time periods by the carriers and the capability to reroute service-outage access.

2. Ensure that contingency plans for telecommunications links, facilities, and data center are finalized and tested and that test results are used to update these plans. Additionally, assurance should be provided that personnel are trained to implement the plans.

Response: OSM concurs with the recommendation and offers the following response:

The OSM Continuity of Operations Plan documents both severity of operational outages and the respective operational contingency site locations. For example, outages affecting only the South Interior Building are to be operationally restored from the Main Interior Building in Washington, D.C. Personnel training, test-plan reviews, test-execution, and lessons learned will be incorporated and updates will be addressed annually.

3. Provide for a secure off-site storage facility that is a least 1 mile from the computer facility.

Response: OSM concurs with this recommendation and offers the following response:

OSM Headquarters, in Washington, D.C., has established the Appalachian Regional Coordinating Center in Greentree, Pennsylvania, a distance of more than 1-mile as the secure offsite storage location.

P. Incident Response Plan and Team

Recommendation:

1. We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop and implement a formal incident response plan and team.

Response: OSM concurs with this recommendation and offers the following response:

OSM is included in the letter of agreement between the Department of the Interior and the Federal Computer Incident Response Capability Program. A copy of this Letter of Agreement is at attachment V. This Letter of Agreement provides Department-wide protection for dealing with criminal activities that pose a threat to critical Federal Information Systems.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Actions Reauired
A.1	Management concurs; additional information needed.	Provide an action plan that addresses the risk assessments for the four mission critical systems that were not included in the response, and include target dates and titles of the officials responsible for implementation.
A.2, A.3, B.1, B.2, C.1, C.2, C.3, D.1, E.1, E.2, E.3, E.4, ES, F.1, F.2, G.1, G.2, G.3, H.1, I.1, J.1, K.4, L.1, L.2, N.1, N.3, and 0.1	Management concurs; additional information needed.	Provide target dates and titles of the officials responsible for implementation.
B.3	Resolved.	We agree with the actions taken.
K.1	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendation will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
K.2, M.1, M.2, N.2, 0.2, 0.3, and P.1	Implemented.	No further response is required.
K.3	Management concurs; additional information needed.	Provide an action plan for developing and implementing policies and procedures to ensure that the system logs are used and that the logs are controlled by personnel independent of the system access control administration function. The plan should include a target date and title of the official responsible for implementation.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL

Internet Complaint Form Address

http://www.oig.doi.gov/hotline_form.html

Within the Continental United States

U.S. Department of the Interior Office of Inspector General 1849 C Street, N.W. Mail Stop 5341 - MIB Washington, D.C. 20240-0001 Our 24-hour Telephone HOTLINE 1-800-424-5081 or (202) 208-5300

TDD for hearing impaired (202) 208-2420

Outside the Continental United States

Caribbean Region

U.S. Department of the Interior Office of Inspector General Eastern Division - Investigations 4040 Fairfax Drive Suite 303 Arlington, Virginia 22203 (703) 235-922 1

Pacific Region

U.S. Department of the Interior Office of Inspector General Guam Field Office 4 15 Chalan San Antonio Baltej Pavilion, Suite 306 Agana, Guam 96911 (67 1) 647-6060



U.S. Department of the Interior Office of Inspector General 1849 C Street, NW Mail Stop 5341- MIB Washington, D.C. 20240-000 1

Toll Free Number 1-800-424-508 1

1

FTS/Commercial Numbers (202) 208-5300 TDD (202) 208-2420

